JABATAN AKAUNTAN NEGARA MALAYSIA

# PROSEDUR PENGURUSAN KESELAMATAN ICT JABATAN AKAUNTAN NEGARA MALAYSIA

# 2019

## (Versi 1.1)

# SEJARAH DOKUMEN

| TARIKH | NAMA DOKUMEN | VERSI | PINDAAN |
|---|---|---|---|
| 7 September 2016 | Prosedur Pengurusan Keselamatan ICT Jabatan Akauntan Negara Malaysia | 1.0 | |
| 25 Januari 2019 | Prosedur Pengurusan Keselamatan ICT Jabatan Akauntan Negara Malaysia | 1.1 | Pengemaskinian Prosedur Pengurusan Keselamatan ICT berdasarkan keperluan pengguna di JANM. |

# PROSEDUR PENGURUSAN KESELAMATAN ICT JANM

## ISI KANDUNGAN

**BAB 4 - PENGURUSAN PANGKALAN DATA**



**BAB 5 - PENGURUSAN KESELAMATAN SISTEM APLIKASI TERAS**



**BAB 6 - PENGURUSAN KESELAMATAN SISTEM APLIKASI SOKONGAN**

**LAMPIRAN 1 - BORANG PENDAFTARAN KAWALAN AKSES ICT**

**LAMPIRAN 2 - BORANG PENAMATAN PERKHIDMATAN KAWALAN AKSES ICT**

**LAMPIRAN 3 - BORANG CHANGE REQUEST**

**LAMPIRAN 4 - SENARAI RUJUKAN DAN PERATURAN**

## BAB 1 - PENGURUSAN DAN PENGGUNAAN E-MEL

### 1.0 PENGENALAN

Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. Setiap penjawat awam mempunyai e-mel rasmi yang digunakan untuk tujuan rasmi dan didaftarkan di bawah agensi Kerajaan. E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

**(a) E-Mel Rahsia Rasmi**

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

**(b) E-Mel Bukan Rahsia Rasmi**

E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi. Semua warga JANM diberi kemudahan e-mel. Setiap warga adalah bertanggungjawab kepada e-mel masing-masing dan perlu mematuhi etika seperti yang dinyatakan dalam Dasar Keselamatan ICT JANM - Perkara 060802 Pengurusan Mel Elektronik (E-mel)

### 2.0 OBJEKTIF

Objektif prosedur ini adalah untuk:

(a) Menerangkan dengan lebih terperinci tatacara penggunaan dan pengurusan e-mel kepada semua warga JANM;

(b) Memastikan kemudahan e-mel JANM digunakan dengan baik dan selamat; dan

(c) Meminimakan sebarang permasalahan berkaitan penggunaan perkhidmatan e-mel.

## 3.0 SKOP

Prosedur ini menerangkan tatacara pengurusan dan pengendalian e-mel di samping peraturan yang perlu diikuti untuk menjamin tahap keselamatan e-mel di JANM.

## 4.0 BIDANG DKICT

Bidang DKICT yang merujuk kepada prosedur ini adalah berikut:

(a) Bidang 6: Pengurusan Operasi dan Komunikasi

- 0605 Housekeeping
- 060802 Pengurusan Mel Elektronik (E-mel)

(b) Bidang 7 : Kawalan Capaian

- 0702 Pengurusan Capaian Pengguna
- 0703 Tanggungjawab Pengguna

## 5.0 PEMAKAIAN

Pemakaian prosedur ini meliputi:

(a) Pentadbir e-mel JANM;

(b) Pengguna emel yang terdiri:

i. Warga JANM;dan

ii. Warga Perkhidmatan Perakaunan Sektor Awam.

## 6.0 PENGECUALIAN

Prosedur ini terpakai untuk semua pihak seperti di para 5.0 kecuali telah mendapat kebenaran bertulis daripada CIO.

## 7.0 PENGURUSAN DAN PENGENDALIAN

| No | Perkara | Peranan |
|---|---|---|
| 7.1 | Pengurusan dan pengendalian | |
| a. | i. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Seksyen/Ketua Unit;<br><br>ii. Memastikan setiap akaun e-mel mempunyai lesen yang sah;<br><br>iii. Memastikan Borang Permohonan e-mel yang lengkap di proses dan akaun e-mel di wujudkan dalam tempoh **tiga (3) hari berkerja**;<br><br>iv. Menamatkan akaun dengan segera (melanggar dasar atau tatacara JANM) atas tujuan keselamatan maklumat menggunakan Borang Penutupan Akaun E-mel;<br><br>v. Akaun e-mel perlu ditamatkan **30 hari** dari tarikh pengguna tamat perkhidmatan di JANM atau dalam sektor awam;<br><br>vi. Akaun e-mel yang tidak diaktif untuk tempoh **90 hari** akan ditamatkan kecuali telah dimaklumkan kepada Pentadbir e-mel;<br><br>vii. Pegawai bertanggungjawab di setiap Bahagian dan Pejabat Perakaunan perlu memaklumkan kepada Pentadbir e-mel **tiga (3) hari bekerja** selepas mana-mana warga JANM yang tamat perkhidmatan / bertukar Jabatan / cuti belajar / cuti bersalin / cuti sakit yang panjang; | Pentadbir e-mel |

| No | Perkara | Peranan |
|---|---|---|
| | viii. Memastikan sistem e-mel berjalan lancar dengan membuat pemantauan operasi harian;<br><br>ix. Memaklumkan **sekurang-kurang satu (1) minggu** lebih awal kepada Pentadbir *Backup & Restore* bagi sebarang peningkatan atau perubahan ke atas perkara berikut:<br><br>a. Sistem Pengoperasian<br><br>b. Pangkalan Data<br><br>c. Sistem Perisian<br><br>Perkara ini perlu di laksanakan bagi memastikan peningkatan tersebut adalah bersesuaian (*compatible*) dengan sistem *backup & restore* di JANM;<br><br>x. Merancang keperluan kapasiti sumber sistem e-mel JANM;<br><br>xi. Memastikan penyenggaraan ke atas sistem e-mel di laksanakan mengikut jadual penyenggaraan pada tahap premium (*premium service*);<br><br>xii. Memaklumkan dan mengambil tindakan ke atas sebarang insiden keselamatan mengikut Prosedur Pengendalian Insiden Keselamatan ICT;<br><br>xiii. Memastikan sistem e-Mel mempunyai sistem tapisan e-mel membuat tapisan untuk e-mel yang mengandungi fail kepilan (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;<br><br>xiv. Menghadkan penghantaran fail kepilan emel kepada 10MB dan menyediakan kaedah bagi penghantaran fail bersaiz lebih 10 MB; | |

| No | Perkara | Peranan |
|---|---|---|
| | xv. Mewujudkan satu akaun e-mel pengujian iaitu “test” dalam domain agensi yang menggunakan kemudahan e-mel jawab automatik (*auto-reply*) bagi maksud pengujian ketersediaan e-mel JANM;<br><br>xvi. Memasang sebarang jenis perisian atau perkakasan penapisan e-mel yang sesuai untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur *spamming*;<br><br>xvii. Perubahan atau pengubahsuaian ke atas sistem e-mel hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai;<br><br>xviii. Perubahan dan/atau pindaan ke atas pakej perisian perlu dikawal dan dihadkan mengikut keperluan;<br><br>xix. Melakukan backup storan e-mel secara harian; dan<br><br>xx. Menyediakan khidmat bantuan bagi penggunaan e-mel JANM. | |
| b. | i. Permohonan akaun e-mel boleh dibuat dengan mengisi borang permohonan e-mel yang boleh diperolehi dari portal rasmi JANM (*www.anm.gov.my*);<br><br>ii. Pengguna baru mesti menukar katalaluan sementara yang diberikan pada login kali pertama;<br><br>iii. Saiz mailbox yang di tetapkan adalah mengikut gred perjawatan seperti berikut: | Pengguna e-mel |

| No | Perkara | Peranan |
|---|---|---|

| Bil | Kumpulan Pengguna | Saiz Mailbox | Saiz Fail Kepilan (*Attachment*) |
|---|---|---|---|
| 1 | Kumpulan Pengurusan Tertinggi (JUSA B dan ke atas) | Tiada had (*Unlimited*) | 10 MB |
| 2 | Kumpulan Pengurusan Tertinggi (JUSA C) | 10 GB | |
| 3 | Kumpulan Pengurusan Dan Profesional (Gred 41 hingga Gred 54) | 2 GB | |
| 4 | Kumpulan Pelaksana | 1.5 GB | |

iv. Kegiatan email pengguna akan dipantau untuk tujuan penguatkuasaan dan dijadikan bahan bukti untuk kes rasmi di mahkamah;

v. Setiap pengguna bertanggungjawab untuk menguruskan e-Mel masing-masing bagi memastikan e-mel yang disimpan tidak melebihi saiz mailbox yang telah diperuntukkan. Sekiranya kapasiti telah digunakan sepenuhnya, e-mel masuk yang baru tidak akan diterima oleh sistem;

vi. E-mel yang telah dibaca atau diambil tindakan hendaklah dipadam atau diarkib agar saiz storan di dalam e-mel server tidak melebihi saiz yang telah diperuntukkan. Ini bertujuan untuk memastikan prestasi server e-mel beroperasi dengan baik pada setiap masa;

vii. Setiap pengguna diberikan storan maya menggunakan CLOUD JANM sebanyak 500MB untuk setiap pengguna khusus bagi penyimpanan fail kepilan emel bersaiz lebih besar dari 10MB;

| No | Perkara | Peranan |
|---|---|---|
| | viii. Memastikan penghantaran e-mel rasmi menggunakan akaun e-mel rasmi JANM ***@anm.gov.my*** dan alamat penerima yang betul. Penggunaan e-mel luar seperti e-mel *Yahoo*, *Gmail*, TMNet dan sebagainya bagi sebarang urusan rasmi adalah tidak dibenarkan;<br><br>ix. E-mel perlu dibuka **sekurang-kurangnya 2 kali setiap hari** dan e-mel penghantar hendaklah dijawab **selewat-lewatnya 1 hari** dari tarikh e-mel diterima;<br><br>x. Sekiranya saiz kepilan (*attachment*) melebihi saiz 10 *Mega byte* (10Mb), kepilan boleh di hantar menggunakan sistem Cloud JANM melalui URL https://cloud.anm.gov.my;<br><br>xi. Menggunakan sistem enkripsi e-mel JANM untuk penghantaran e-mel **Terhad** atau **Sulit** sebelum di hantar kepada penerima bagi menjamin keselamatan dan mengelakkan kebocoran maklumat terperingkat;<br><br>xii. Memastikan setiap fail yang dimuat turun bebas daripada virus sebelum digunakan;<br><br>xiii. Pengguna hendaklah membuat salinan dan menyimpan fail kepilan ke dalam satu *folder* berasingan dari setiap e-mel yang penting bagi tujuan *backup* jika berlaku sebarang masalah kepada cakera keras komputer;<br><br>xiv. Webmail JANM (mail.anm.gov.my) juga boleh dicapai oleh semua pengguna yang ingin membuat capaian e-mel di dalam atau di luar pejabat;<br><br>xv. Penggunaan huruf besar kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika sebaliknya menggunakan bahasa yang ringkas, betul dan sopan; | |

| No | Perkara | Peranan |
|---|---|---|
| | xvi. Bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel dalam akaun sendiri;<br><br>xvii. Kemudahan 'salinan kepada (cc)' boleh digunakan sekiranya e-mel perlu dimaklumkan kepada penerima lain. Bagaimanapun, penggunaan 'blind cc' (bcc) tidak digalakkan;<br><br>xviii. Memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan;<br><br>xix. Kemudahan penghantaran e-mel jawab automatik semasa berada di luar pejabat bagi tempoh waktu yang panjang adalah digalakkan;<br><br>xx. Kemudahan e-mel tidak boleh digunakan untuk menghantar bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian, jenayah, cetak rompak atau apa-apa maklumat yang menjejaskan reputasi JANM dan Perkhidmatan Awam;<br><br>xxi. Kemudahan e-mel rasmi tidak boleh digunakan untuk tujuan peribadi, komersial atau politik;<br><br>xxii. Tidak dibenarkan menghantar e-mel sampah (*junk mail*) dan e-mel *spam* serta menyebarkan kod perosak seperti *virus*, *worm,* dan *trojan horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;<br><br>xxiii. Tidak dibenarkan menyimpan dan memuat turun bahan yang mempunyai hakcipta, termasuk yang dimuat turun dari Internet atau menyebarkan kepada pihak lain tanpa mendapat kebenaran terlebih dahulu daripada pemilik hak cipta yang berkenaan; | |

| No | Perkara | Peranan |
|---|---|---|
| | xxiv. Membuat aduan atau laporan rasmi kepada Unit Aplikasi Gunasama (UAG) jika menerima kandungan email yang disertakan dengan bahan yang terlarang;<br><br>xxv. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akses akaun kepada orang lain untuk menjawab e-mel bagi pihaknya;<br><br>xxvi. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah.<br><br>xxvii. Rekod e-mel berkaitan sesuatu keputusan penting atau tindakan yang telah diambil hendaklah dicetak dan difailkan;<br><br>xxviii. Rahsiakan dan kukuhkan kata laluan e-mel mengikut prosedur kawalan capaian;<br><br>xxix. Kata laluan hendaklah ditukar setiap **6 bulan**. Panjang kata laluan mestilah **sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus**. Contohnya P@$$w0rd123 dan D3$kn0w123; dan<br><br>xxx. Menukar kata laluan apabila disyaki berlakunya kebocoran atau dikompromi. Kata laluan hendaklah diingat dan **TIDAK BOLEH** didedahkan dengan apa cara sekalipun. | |

## BAB 2 - PENGURUSAN RANGKAIAN DAN KESELAMATAN ICT

### 1.0 PENGENALAN

Prosedur ini diwujudkan adalah sebagai garis panduan dalam pengurusan dan pengendalian rangkaian dan keselamatan ICT di JANM.

### 2.0 OBJEKTIF

Kawalan terhadap penggunaan rangkaian perlu dibuat untuk menjamin kerahsiaan, integriti dan kesediaannya. Ia bertujuan bagi memastikan maklumat yang disalurkan melaluinya diterima, tidak tergugat akibat ancaman keselamatan rangkaian atau penggunaan rangkaian yang tidak dibenarkan.

### 3.0 SKOP

Prosedur ini menerangkan tatacara perolehan, konfigurasi, pengoperasian dan penyenggaraan peralatan rangkaian dan keselamatan bagi pentadbir rangkaian, pentadbir keselamatan serta peraturan yang perlu diikuti oleh pihak ketiga dan pengguna yang menggunakan kemudahan rangkaian di JANM.

### 4.0 BIDANG DKICT

Bidang DKICT yang merujuk kepada prosedur ini adalah berikut:

(a) Bidang 02: Organisasi Keselamatan

- 0201 Infrastruktur Organisasi Dalaman
- 020107 Jawatankuasa Keselamatan ICT JANM
- 020108 Pasukan Tindak Balas Insiden Keselamatan ICT

(b) Bidang 05: Keselamatan Fizikal Dan Persekitaran

- 0502 Keselamatan Peralatan
- 050201 Peralatan ICT

- 050202 Pusat Data
- 050204 Media Tandatangan Digital
- 050205 Media Perisian dan Aplikasi
- 050206 Penyenggaraan Perkakasan
- 050207 Peralatan di Luar Premis
- 050208 Pelupusan Perkakasan
- 0503 Keselamatan Persekitaran
- 050303 Kabel

(c) Bidang 06: Pengurusan Operasi dan Komunikasi

- 0601 Pengurusan Prosedur Operasi
- 060103 Pengasingan Tugas dan Tanggungjawab
- 0606 Pengurusan Rangkaian
- 060601 Kawalan Infrastruktur Rangkaian
- 0610 Pemantauan
- 061003 Sistem Log

(d) Bidang 07: Kawalan Capaian

- 0702 Pengurusan Capaian Pengguna
- 070201 Akaun Pengguna
- 070202 Hak Capaian
- 070204 Semakan Capaian Pengguna
- 0704 Kawalan Capaian Rangkaian
- 070401 Capaian Rangkaian
- 070402 Infrastruktur Rangkaian
- 070403 Capaian Internet
- 0706 Kawalan Capaian Aplikasi dan Maklumat
- 070601 Capaian Aplikasi dan Maklumat
- 070602 Infrastruktur Kekunci Awam (PKI)
- 070603 Kawalan Capaian Perbankan Internet
- 070604 Pengkomputeran Awan (Cloud Computing)

(e) Bidang 09: Pengurusan Pengendalian Insiden Keselamatan

- 0901 Mekanisme Pelaporan Insiden Keselamatan ICT

## 5.0 PEMAKAIAN

Prosedur ini perlu dipatuhi oleh semua pengguna rangkaian JANM kecuali dengan kebenaran bertulis daripada ICTSO.

## 6.0 PENGECUALIAN

Prosedur ini terpakai untuk semua pihak seperti di para 5.0 kecuali telah mendapat kebenaran bertulis daripada CIO.

## 7.0 PENGURUSAN DAN PENGENDALIAN

| No | Perkara | Peranan |
|---|---|---|
| 7.1 Perolehan | | |
| a. | Sebelum mengemukakan cadangan untuk sebarang perolehan berkaitan dengan peralatan rangkaian dan keselamatan ICT JANM, kajian perlu dibuat untuk menentukan kesesuaian teknologi, keserasian, dan nilai pasaran sesuatu peralatan, perisian, perkhidmatan atau perundingan yang perlu diperoleh. | Pentadbir |
| b. | Semua peralatan/perisian rangkaian dan keselamatan mempunyai lesen yang sah dan bukti lesen tersebut perlu disimpan dalam *warchest*. | Pentadbir |
| c. | Khidmat nasihat dalam hal ehwal berkaitan infrastruktur, pengoperasian dan keselamatan rangkaian di ibu pejabat dan semua pejabat perakaunan perlu diberikan sebelum perolehan berkaitan rangkaian dan keselamatan ICT dibuat. | Pentadbir |
| d. | Piawaian yang berkaitan dengan operasi sesuatu peralatan perlu dipatuhi dan disebutkan dalam spesifikasi perolehan. Contohnya, sokongan terhadap protokol IPv6. | Pentadbir |

| | | |
|---|---|---|
| 7.2 Pemasangan IPS | | |
| a. | Sekatan dibuat berdasarkan alamat IP penceroboh pada IPS sekiranya menerima laporan daripada GCERT, MyGSOC, sumber yang dipercayai atau hasil pemantauan mengenai IP yang menceroboh atau membuat percubaan menceroboh ke sistem-sistem JANM. | Pentadbir |
| 7.3 Pemasangan Firewall | | |
| a. | Penetapan untuk routing, peraturan tapisan, translasi alamat IP dalam ke IP luar (*Network Address Translation*) dibuat setelah kelulusan diperoleh dan diletakkan dengan penerangan (*description*) yang ringkas serta mudah difahami oleh pentadbir. Penetapan dibuat berdasarkan maklumat yang terdapat dalam Borang Pengurusan Perubahan (Lampiran 3). | Pentadbir |
| 7.4 Pemasangan Pengimbang Beban (Load Balancer) | | |
| a. | Fungsi pengimbang beban adalah untuk mengurangkan kepadatan trafik, jika terdapat kepadatan pada sesuatu server, maka permintaan berikutnya akan dialihkan ke server yang lain**.** Pengagihan ini bertujuan supaya server-server yang mempunyai fungsi yang sama dan bertujuan untuk kesediaan yang tinggi menerima beban yang seimbang. | Pentadbir |
| 7.5 Pemasangan Switch | | |
| a. | Melaksanakan pengasingan rangkaian kepada segmen yang berbeza (VLAN) agar trafik berbentuk *broadcast* pada sesuatu segmen tidak menjejaskan prestasi rangkaian di segmen yang lain. | Pentadbir |
| b. | Setiap port pada switch adalah dipadankan dengan alamat MAC (*media access control*) sesuatu peralatan seperti PC. Hanya 2 alamat MAC yang dibenarkan menggunakan sesuatu port rangkaian dalam sesuatu masa. Switch dikonfigurasi untuk pengasingan rangkaian menggunakan segmen yang berbeza (VLAN). | Pentadbir |

| | | |
|---|---|---|
| 7.6 Pemasangan CRL Server Untuk Menyokong Tandatangan Digital | | |
| a. | Fail CRL atau *Certificate Revocation List* mestilah memuatkan sijil yang telah dibatalkan oleh pihak berkuasa pemerakuan (CA) dan boleh dimuat turun daripada server CRL CA. Fail CRL ini perlu dikemaskini setiap 48 jam. | Pentadbir |
| 7.7 Pemasangan Rangkaian Tanpa Wayar | | |
| a. | Memastikan semua peranti infrastruktur Rangkaian Tanpa Wayar yang disambungkan ke rangkaian JANM<br><br>• Mematuhi piawaian yang ditetapkan dalam Standard Komunikasi Tanpa Wayar.<br>• Menggunakan protokol dan infrastruktur pengesahan yang diluluskan.<br>• Menggunakan protokol penyulitan JANM yang diluluskan.<br>• Peranti berupaya menyimpan alamat MAC perkakasan yang menggunakan rangkaian tanpa wayar. | Pentadbir |
| b. | Profail yang dicipta perlu dibahagikan kepada pengunjung JANM (JANM-Guest), pengguna dalaman (JANM-Staff) dan pembekal (JANM-Vendor) agar pengguna rangkaian tanpa wayar JANM yang bukan kakitangan Kerajaan hanya dapat melayari internet sahaja. Manakala profail JANM-Staff digunakan oleh pegawai dan kakitangan JANM untuk membuat capaian ke internet dan capaian rangkaian tanpa wayar sehingga ke *host* dalaman. Sebelum penggunaan rangkaian tanpa wayar, *username* dan *password* perlu dimasukkan melalui *browser* untuk menentukan bahawa pengguna telah dibenarkan menggunakan rangkaian tanpa wayar JANM. *Username* dan *password* untuk profail JANM-Guest dipaparkan di bilik-bilik mesyuarat dan ruang berkumpul bagi pengunjung yang berurusan dengan JANM. | Pentadbir |

| | | |
|---|---|---|
| 7.8 Pemantauan Pengggunaan Sumber Rangkaian dan Keselamatan | | |
| a. | Kajian perlu dibuat dari semasa ke semasa untuk memastikan semua peralatan rangkaian dan keselamatan berada di bawah garisan threshold. Bagi penggunaan yang menghampiri atau melepasi garisan threshold, maka peningkatan kapasiti perlu dirancang dan dilaksanakan. | Pentadbir |
| 7.9 Pengggunaan Rangkaian | | |
| a. | Trafik keluar dan masuk ke rangkaian JANM, *server farm*/vlan user mesti melalui firewall. | Pentadbir |
| b. | Pengagihan alamat IP perlu dibuat menggunakan *Dynamic Host Configuration Protocol* (DHCP). | Pentadbir |
| c. | Log-log untuk setiap peralatan rangkaian dan keselamatan mestilah diaktifkan, disimpan selama sekurang-kurangnya 6 bulan atau mengikut keperluan dan dipantau dari semasa ke semasa. | Pentadbir |
| d. | Perisian untuk peralatan rangkaian dan keselamatan mestilah dinaik taraf ke versi terkini untuk mengukuhkan ciri-ciri keselamatan peralatan tersebut. | Pentadbir |
| e. | Konfigurasi untuk setiap peralatan rangkaian dan keselamatan harus dibuat salinan backup setiap kali terdapat perubahan atau penetapan konfigurasi yang baru atau peningkatan perisian peralatan. | Pentadbir |
| f. | Peralatan rangkaian dan keselamatan tidak boleh dibawa keluar dari lokasi pemasangannya kecuali mendapat kelulusan daripada timbalan pengarah seksyen perkhidmatan ICT. | Semua |

| | | |
|---|---|---|
| g. | Mekanisme keselamatan rangkaian meliputi *intrusion prevention system* (IPS)/*intrusion detection system* (IDS), firewall dan antivirus hendaklah dipasang untuk melindungi server-server kritikal JANM. | Pentadbir |
| h. | Hanya PC atau peranti elektronik yang dibenarkan sahaja boleh membuat sambungan pada *virtual local area network* (vlan) yang telah ditetapkan. | Pentadbir |
| i. | Perisian *Content Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan. | Pentadbir |
| j. | Penggunaan teknologi (*packet shaper*) untuk mengawal aliran trafik adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang optimum dan lebih berkesan. | Pentadbir |
| k. | Maklumat berkaitan rangkaian JANM seperti alamat IP, konfigurasi, rekabentuk adalah tidak dibenarkan sama sekali didedahkan kepada pihak luar. | Semua |
| l. | Pengguna dilarang memuat naik, memuat turun, menyimpan dan menggunakan sebarang aplikasi seperti permainan elektronik, video, perjudian, lagu material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah kerana boleh menjejaskan tahap capaian internet; dan | Pengguna |
| m. | Pengguna menghantar, menyebar, menyimpan atau menerima pesanan atau maklumat palsu, ugutan, bahan atau pesanan yang menjadi kesalahan dan sensitif kepada perkauman, kebudayaan, seksual atau kepentingan awam. | Pengguna |

| | | |
|---|---|---|
| 7.10 Kawalan Akses | | |
| a. | Semua pengguna yang memiliki akaun memasuki peralatan rangkaian dan keselamatan mestilah mengisi dan menandatangani Borang Pendaftaran Kawalan Akses ICT (Lampiran 1) untuk tujuan kawalan akses ke atas peralatan. | Semua |
| b. | Akaun yang telah diluluskan dalam Borang Pendaftaran Kawalan Akses ICT (Lampiran 1) perlu dicipta dan dimaklumkan kepada pemohon. | Pentadbir |
| c. | Pemadaman akaun pengguna dan melengkapkan Borang Penamatan Perkhidmatan untuk Kawalan Akses ICT (Lampiran 2) apabila dimaklumkan akaun tersebut tidak diperlukan lagi perlu dibuat. | Pentadbir |
| d. | Semua pengguna perlu membaca, memahami dan menandatangani Surat Akuan Pematuhan DKICT JANM | Semua |
| e. | Akaun pentadbir yang dibenarkan akses untuk membuat perubahan konfigurasi pada peralatan rangkaian dan keselamatan perlu dimasukkan dalam kumpulan (*organizational group*) dalam *Active Directory* bagi peralatan rangkaian dan keselamatan. | Pentadbir |
| 7.11 Perlindungan Rangkaian Daripada Perisian Berbahaya | | |
| a. | Mengimbas semua kandungan storan luaran dengan antivirus jika mengesyaki kandungan storan dijangkiti perisian berbahaya atau virus. | Pengguna |
| b. | Memastikan tiada sambungan perkakasan yang mencurigakan pada port USB komputer pejabat. | Pengguna |

| | | |
|---|---|---|
| c. | Penggunaan *modem, wireless access point* dan *broadband* persendirian yang dihubungkan dengan rangkaian JANM adalah dilarang sama sekali. | Semua |
| d. | Perisian *sniffer* atau *network analyzer* adalah dilarang sama sekali dipasang di mana-mana pc atau notebook kecuali pada PC yang digunakan oleh pentadbir rangkaian dan keselamatan. | Semua |
| 7.12 Imbasan Kelemahan Sistem | | |
| a. | Perisian pengesan kelemahan perlu dipasang dalam segmen rangkaian yang sama dengan server-server atau host yang akan diimbas. | Pentadbir |
| b. | Bagi membuat penilaian kelemahan sistem menggunakan perisian ini, pentadbir perlu menetapkan polisi imbasan, melaksanakan imbasan pada *host* sasaran dan menjanakan laporan kelemahan yang dijumpai untuk diambil tindakan oleh pentadbir sistem berkenaan. | Pentadbir |
| c. | Imbasan mesti dilaksanakan semasa sistem kurang dicapai jika memberi kesan terhadap prestasi sistem. | Pentadbir |
| 7.13 Penyenggaraan Rangkaian dan Keselamatan | | |
| a. | Sebarang penyenggaraan yang memerlukan rangkaian ditutup dan tidak boleh dicapai dalam tempoh tertentu perlu dirancang dan mendapat persetujuan daripada pentadbir sistem-sistem lain terlebih dahulu dan seterusnya dimaklumkan kepada pengguna. | Pentadbir |
| b. | Perjanjian Tahap Perkhidmatan (*Service Level Agreement*) perlu wujud antara JANM dengan pembekal peralatan rangkaian yang kritikal seperti router, firewall dan switch agar sebarang kerosakan pada peralatan tersebut dapat dipulihkan dalam jangka waktu tidak melebihi 2 hari bekerja. | Pentadbir & Pihak Ketiga |

| | | |
|---|---|---|
| c. | Penyenggaraan mencegah boleh perlu dilaksanakan untuk peralatan kritikal untuk mengekalkan jangka hayat dan penggunaan peralatan secara optimum. | Pentadbir |
| 7.14 Kawalan Perubahan | | |
| a. | Borang Pengurusan Perubahan (Lampiran 3) perlu digunakan untuk mencatat permohonan, kelulusan dan pelaksanaan perubahan yang dibuat pada konfigurasi, perisian atau perkakasan (*hardware*) rangkaian dan keselamatan. | Pentadbir |
| b. | Bagi kawalan perubahan ke atas peralatan rangkaian dan keselamatan MyGov*Net yang dibekalkan oleh MAMPU, permohonan perubahan hendaklah menggunakan sistem https://mygovosf.gitn.net.my/login.php. | Pentadbir |
| 7.15 Pengurusan Kata Laluan | | |
| | Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan seperti berikut:<br><br>a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi;<br>b) Menukar kata laluan apabila disyaki berlakunya kebocoran atau dikompromi;<br>c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus;<br>d) Kata laluan hendaklah diingat dan TIDAK BOLEH didedahkan dengan apa cara sekalipun;<br>e) Mengaktifkan kata laluan windows dan *screen saver* JANM terutamanya pada PC pengguna;<br>f) Pengguna hendaklah memastikan kata laluan berlainan daripada pengenalan identiti pengguna; | Pentadbir |

| | | |
|---|---|---|
| | g) Memastikan sistem berupaya menamatkan sesi dalam sesuatu tempoh masa tertentu apabila sistem tidak digunakan; dan<br>h) Memastikan penukaran kata laluan semasa login kali pertama dan set semula, tempoh penukaran, bilangan percubaan kemasukan kata laluan serta penggunaan semula kata laluan terdahulu yang digunakan dilaksanakan bersesuaian dengan keperluan sistem. | |
| 7.16 Pelaporan Insiden Keselamatan ICT | | |
| a. | Pelaporan insiden keselamatan ICT mestilah mengikut Surat Pekeliling Am Bilangan 4 Tahun 2006. | Pentadbir |

## BAB 3 - PENGURUSAN PERKAKASAN DAN PERISIAN ICT SERTA PUSAT DATA

### 1.0 PENGENALAN

Prosedur ini diwujudkan adalah sebagai garis panduan dalam pengurusan dan pengendalian perkakasan dan perisian ICT serta Pusat Data di JANM.

### 2.0 OBJEKTIF

Objektif prosedur ini adalah untuk:

(a) Menerangkan dengan lebih terperinci tatacara pengurusan dan pengendalian perkakasan dan perisian ICT serta pusat data kepada semua warga JANM dan pihak luar yang berkenaan; dan

(b) Memastikan pengurusan dan pengendalian perkakasan, perisian dan pusat data adalah mengikut tatacara yang betul untuk menjamin kesediaan dan keselamatan maklumat.

### 3.0 SKOP

Prosedur ini menerangkan tatacara perolehan, pengagihan, pengoperasian, penyenggaraan dan pelupusan perkakasan/perisian ICT dan pusat data di samping peraturan yang perlu diikuti untuk menjamin tahap keselamatan perkakasan, perisian dan pusat data di JANM.

### 4.0 BIDANG DKICT

Bidang DKICT yang merujuk kepada prosedur ini adalah berikut:

(a) Bidang 05: Keselamatan Fizikal dan Persekitaran

- 050201 Perkakasan ICT

- 050202 Pusat Data
- 050203 Media Storan
- 050206 Penyenggaraan Perkakasan
- 050208 Pelupusan Perkakasan

(b) Bidang 06 : Pengurusan Operasi dan Komunikasi

- 060301 Perancangan Kapasiti
- 060502 Housekeeping Storan
- 0607 Pengurusan Media
- 060801 Pertukaran Maklumat
- 0610 Pemantauan

## 5.0 PEMAKAIAN

Pemakaian prosedur ini meliputi:

(a) Pentadbir perkakasan/perisian ICT dan pusat data;
(b) Pengguna iaitu warga JANM; dan
(c) Pihak ketiga iaitu pihak luar yang menjalankan perkhidmatan dengan JANM.

## 6.0 PENGECUALIAN

Prosedur ini terpakai untuk semua pihak seperti di para 5.0 kecuali telah mendapat kebenaran bertulis daripada CIO.

## 7.0 PENGURUSAN DAN PENGENDALIAN PERKAKASAN DAN PERISIAN ICT

| No | Perkara | Peranan |
|---|---|---|
| 7.1 Perolehan | | |
| | i. Perolehan perkakasan/perisian ICT hendaklah mengikut tatacara perolehan semasa yang berkuat kuasa.<br><br>ii. Proses utama perolehan adalah seperti berikut :<br>• Perancangan perolehan;<br>• Pelaksanaan perolehan;<br>• Penilaian perolehan;<br>• Pemantauan dan pelaksanaan projek; dan<br>• Pengurusan dan pentadbiran kontrak. | Pentadbir Perkakasan & Perisian ICT |
| 7.2 Pengagihan | | |
| | i. Memastikan pengagihan perkakasan dan perisian ICT yang disediakan mencukupi, memenuhi keperluan operasi perkhidmatan serta dilaksanakan dengan cekap dan berkesan. Pengagihan selain dari yang dinyatakan di para ini, hendaklah mengikut keperluan kerja dan kapasiti semasa dengan perakuan dan mendapat kelulusan daripada pengurus ICT/ICTSO.<br><br>ii. Pengagihan perkakasan dan perisian ICT di JANM adalah seperti berikut :<br><br>(a) Komputer Desktop (PC)<br>• Pegawai Kumpulan Pengurusan Tertinggi;<br>• Pegawai kumpulan Pengurusan dan Profesional; dan<br>• Kumpulan Pelaksana.<br><br>(b) Komputer Riba:<br>• Pegawai Kumpulan Pengurusan Tertinggi; | Pentadbir Perkakasan & Perisian ICT |

| No | Perkara | Peranan |
|---|---|---|
| | • Pengarah Negeri/Cawangan; dan<br>• Setiap Unit/Seksyen di JANM (secara gunasama).<br><br>(c) Peranti mudah alih<br><br>• Pegawai Kumpulan Pengurusan Tertinggi;<br>• Pengarah Negeri/Cawangan; dan<br>• Pegawai dengan jawatan Gred 54.<br><br>(d) Pencetak<br><br>• Pegawai Kumpulan Pengurusan Tertinggi dibekalkan dengan pencetak warna;<br>• Pegawai Kumpulan Pengurusan dan Profesional Gred 48 dan ke atas dibekalkan dengan pencetak hitam putih;<br>• Pegawai Kumpulan Pengurusan dan Profesional Gred 44 dan ke bawah dibekalkan dengan pencetak hitam putih secara gunasama; dan<br>• Setiap bahagian di Ibu Pejabat, JANM Negeri dan Cawangan dibekalkan dengan pencetak hitam putih dan pencetak warna berkapasiti tinggi mengikut keperluan dengan mendapat perakuan Pengurus ICT dan kelulusan ICTSO.<br><br>(e) Pengimbas<br><br>• Pejabat Pengurusan Tertinggi, bahagian, JANM Negeri dan Cawangan layak dibekalkan pengimbas bersaiz A3/A4; dan<br>• Pengimbas berteknologi tinggi dibekalkan mengikut keperluan tugasan rasmi dan dengan perakuan Pengurus ICT. | |

| No | Perkara | Peranan |
|---|---|---|
| | (f) Sistem Pengoperasian server<br>• Microsoft Windows;<br>• Linux; dan<br>• Unix.<br><br>(g) Aplikasi Desktop dan Komunikasi<br>• Warga kerja JANM yang terlibat dengan kerja-kerja seperti urusan pentadbiran, kewangan dan pembangunan projek layak dibekalkan dengan perisian Microsoft Office;<br>• Setiap bahagian di Ibu Pejabat, JANM Negeri dan Cawangan dibekalkan dengan perisian Microsoft Visio, Microsoft Project dan Dewan Eja;<br>• Perisian grafik Adobe Photoshop hanya dibekalkan kepada warga kerja yang terlibat dengan kerja-kerja penyuntingan dan pembangunan multi media;<br>• Perisian Macromedia Director hanya dibekalkan kepada bahagian/unit yang terlibat dalam pembangunan aplikasi berasaskan web;<br>• Perisian Adobe Master dalam persekitaran Macintosh dibekalkan kepada bahagian/unit yang terlibat dalam penyediaan penyata kewangan kerajaan persekutuan; dan<br>• Aplikasi komunikasi seperti web based email, Internet Explorer, Firefox, Google Chrome dibekalkan kepada semua warga JANM yang berkaitan.<br><br>iii. Semua perkakasan dan perisian ICT yang telah diagih hendaklah direkod dengan sempurna serta dilabel mengikut *standard* yang ditetapkan. | |

| No | Perkara | Peranan |
|---|---|---|
| 7.3 Pengurusan | | |
| a. | Perkakasan dan Perisian<br>i. Perkakasan ICT yang hendak dibawa keluar dari premis JANM perlulah mendapat kebenaran Pentadbir perkakasan/perisian ICT dan direkodkan bagi tujuan pemantauan;<br>ii. Tidak dibenarkan membuat penambahan, menanggal atau mengganti perkakasan ICT yang telah ditetapkan;<br>iii. Kedudukan perkakasan dari tempat asal tidak boleh diubah kecuali telah mendapat kebenaran Pentadbir Perkakasan/Perisian ICT;<br>iv. Sebarang instalasi perisian tambahan hendaklah mendapat kebenaran Pentadbir Perkakasan/Perisian ICT; dan<br>v. Tidak dibenarkan menampal sebarang pelekat selain untuk tujuan rasmi. | Pengguna |
| b | Kawasan Kerja<br>i. Memastikan semua maklumat sensitif/sulit dalam bentuk salinan atau elektronik adalah selamat apabila hendak meninggalkan kawasan kerja.<br>ii. Komputer mesti ditutup (logoff) sepenuhnya pada akhir hari kerja.<br>iii. Komputer riba mestilah dikunci dengan kabel mengunci atau dikunci dalam laci.<br>iv. Kata laluan tidak boleh ditulis, dipamer dan diletakkan pada komputer atau kawasan kerja.<br>v. Cetakan yang mengandungi maklumat Terhad atau Sensitif/Sulit hendaklah dikeluarkan dengan segera dari pencetak.<br>vi. Apabila pelupusan Dokumen Terhad atau Sensitif/Sulit hendaklah dirincih.<br>vii. Media storan seperti CDROM, DVD atau USB disimpan di tempat yang selamat. | Pengguna |

| No | Perkara | Peranan |
|---|---|---|
| c. | i. Instalasi perisian hanya dilakukan ke atas perkakasan yang dibekalkan oleh JANM dan memastikan perisian yang dipasang adalah perisian yang sah;<br>ii. Setiap perisian perlu bebas daripada kelemahan, keterdedahan, virus dan aturcara tidak sah;<br>iii. Semua maklumat perkakasan/perisian ICT yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal dan dikemaskini dari semasa ke semasa mengikut keperluan;<br>iv. Latihan perlu diberikan kepada pengguna bagi perisian yang baru dipasang atau dipertingkatkan;<br>v. Semua perkakasan ICT (*server dan storage*) yang digunakan secara berterusan perlu diletakkan di dalam Pusat Data; dan<br>vi. Memastikan perkakasan dan perisian berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan;<br>vii. Semua perkakasan/perisian ICT hendaklah disimpan atau diletakkan di tempat yang sesuai, bersih dan mempunyai ciri-ciri keselamatan bagi melindungi daripada kecurian, penyalahgunaan atau pengubahsuaian tanpa kebenaran;<br>viii. Melakukan penyulitan dan penyahsulitan terhadap perkakasan dan perisian yang melibatkan maklumat terperingkat atau maklumat sulit; dan<br>ix. Mengadakan salinan atau penduaan (*backup*) pada maklumat yang disimpan dalam perkakasan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data dan disimpan mengikut prosedur *backup* yang telah ditetapkan. | Pentadbir Perkakasan & Perisian ICT |
| d. | i. Perkakasan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;<br>ii. Penggunaan kata laluan pada setiap perkakasan ICT (server dan komputer) adalah diwajibkan; dan | Pentadbir Perkakasan & Perisian ICT/ Pengguna |

| No | Perkara | Peranan |
|---|---|---|
| | iii. Kawalan perkakasan dan perisian daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan. | |
| 7.4 Penyenggaraan | | |
| | i. Semua perkakasan/perisian ICT hendaklah disenggara mengikut skop dan jadual yang ditetapkan atau yang dipersetujui;<br>ii. Penyenggaraan hendaklah dilakukan oleh kakitangan atau pihak yang dibenarkan sahaja;<br>iii. Semua penyenggaraan mestilah mendapat kebenaran daripada Pengurus ICT atau pegawai yang diberi kuasa;<br>iv. Menyemak dan menguji semua perkakasan/perisian ICT sebelum dan/atau selepas proses penyenggaraan;<br>v. Semua kerja penyenggaraan hendaklah direkodkan di dalam borang rekod kerja/*Service Report* dan disahkan oleh pegawai yang berkenaan;<br>vi. Penggantian alat ganti/ komponen perkakasan ICT hendaklah mendapat kebenaran Pentadbir perkakasan/perisian ICT. Maklumat penggantian hendaklah dikemaskini di Bahagian B dalam rekod KEW.PA-2 atau KEW.PA-3 perkakasan tersebut;<br>vii. Semua perisian hendaklah dipertingkatkan (*upgrade*) dari semasa ke semasa bagi memastikan versi yang terkini dan mengikut keperluan;<br>viii. Sebarang *update (patches* dan *firmware)* yang hendak dipasang pada server hendaklah diuji terlebih dahulu sebelum di pasang ke persekitaran *live* server; dan<br>ix. Sebarang peningkatan atau kemaskini *patches* daripada perisian sedia ada perlu dilaksanakan sebaik mungkin dan perisian berfungsi mengikut *standard* yang ditetapkan. | Pentadbir Perkakasan & Perisian ICT |

| No | Perkara | Peranan |
|---|---|---|
| 7.5 Pelupusan | | |
| a. | i. Pelupusan perkakasan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; | Pegawai Aset/ Pentadbir Perkakasan & Perisian ICT |
| b. | i. Mengenal pasti aset-aset yang boleh dilupuskan;<br>ii. Semua kandungan perkakasan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degaussing* atau pembakaran; dan<br>iii. Perkakasan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan perkakasan tersebut. | Pentadbir Perkakasan & Perisian ICT |
| c. | i. Sekiranya maklumat yang akan dihapuskan perlu disimpan, pengguna hendaklah membuat penduaan; dan<br>ii. Perkakasan ICT yang akan dilupuskan tidak boleh dipindahkan ke lokasi lain sehingga pelupusan selesai. | Pengguna |

## 8.0 PENGURUSAN DAN PENGENDALIAN PUSAT DATA

| No | Perkara | Peranan |
|---|---|---|
| 8.1 Perolehan | | |
| | i. Perolehan peralatan Pusat Data hendaklah mengikut tatacara tatacara perolehan semasa yang berkuat kuasa.<br><br>ii. Proses utama perolehan adalah seperti berikut :<br>• Perancangan perolehan;<br>• Pelaksanaan perolehan;<br>• Penilaian perolehan;<br>• Pemantauan dan pelaksanaan projek; dan<br>• Pengurusan dan pentadbiran kontrak. | Pentadbir Pusat Data |
| 8.2 Pengagihan | | |
| | i. Pengagihan peralatan Pusat Data hendaklah mengikut keperluan semasa dengan perakuan dan kelulusan daripada ICTSO; dan<br>ii. Memastikan semua peralatan utiliti Pusat Data direkod dengan sempurna serta dilabel mengikut *standard* yang ditetapkan. | Pentadbir Pusat Data |
| 8.3 Pengurusan | | |
| | i. Pusat Data dilengkapkan dengan peralatan *Uninterruptible Power Supply* (UPS), bekalan kuasa elektrik skunder (*Generator-Set*), *voltage stabilizer*, sistem penghawa dingin dengan sudu di antara 19°C hingga 24°C dengan kelembapan pada tahap 60% hingga 70%, sistem pencegahan kebakaran, sistem keselamatan pintu utama serta sistem pemantauan seperti sistem pemantauan persekitaran (*Environmental Monitoring System*) untuk mengesan asap, haba dan kebocoran air;<br>ii. Memastikan semua perkakasan berada dalam keadaan baik dan sentiasa boleh guna, selamat dari segi logikal dan fizikal | Pentadbir Pusat Data |

| No | Perkara | Peranan |
|---|---|---|
| | serta mempunyai ruang yang mencukupi untuk menempatkan perkakasan yang berkaitan;<br>iii. Melaporkan sebarang kerosakan peralatan pusat data kepada Meja Bantuan (*helpdesk*) atau Pihak Ketiga;<br>iv. Memastikan semua permohonan penempatan, peralihan dan pengeluaran sebarang perkakasan dalam pusat data perlu mendapat kelulusan Pentadbir Pusat Data;<br>v. Mengemaskini *layout* pusat data dan didokumentasikan sekiranya perlu;<br>vi. Memastikan semua pintu dan tingkap sentiasa ditutup dan Sistem Pintu Keselamatan berfungsi dengan baik;<br>vii. Memastikan pusat data mempunyai sistem pendawaian yang kemas, selamat dan mengikut spesifikasi yang dibenarkan;<br>viii. Memastikan pusat data sentiasa bersih dan tidak terdedah kepada habuk; dan<br>ix. Melaksanakan kesinambungan perkhidmatan pusat data termasuk pemulihan pusat data sekiranya berlaku bencana. | |
| 8.4 Penyenggaraan | | |
| | i. Memastikan pusat data disenggara mengikut jadual yang telah ditetapkan;<br>ii. Semua kerja penyenggaraan hendaklah direkodkan di dalam borang rekod kerja/*Service Report* dan disahkan oleh pegawai berkenaan;<br>iii. Memantau kerja penyelenggaraan yang dilakukan oleh Pihak Ketiga;<br>iv. Memastikan kakitangan JANM atau pihak ketiga mendapat kebenaran daripada Pentadbir Pusat Data sebelum memasuki pusat data dan merekod maklumat ke dalam Rekod masuk/keluar; dan<br>v. Memastikan rekod masuk/keluar di pusat data diselenggara. | Pentadbir Pusat Data |

| No | Perkara | Peranan |
|---|---|---|
| 8.5 Pelupusan | | |
| a. | i. Pelupusan peralatan pusat data hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; | Pegawai Aset/ Pentadbir Pusat Data |
| b. | i. Mengenal pasti aset-aset yang boleh dilupuskan;<br>ii. Perkakasan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan perkakasan tersebut; | Pentadbir Pusat Data |
| c. | i. Perkakasan ICT yang akan dilupuskan tidak boleh dipindahkan ke lokasi lain sehingga pelupusan selesai. | Pengguna |

# BAB 4 - PENGURUSAN PANGKALAN DATA

## 1.0 PENGENALAN

Pangkalan data merupakan satu sistem simpanan data yang tersusun dalam bentuk elektronik bagi membolehkan proses capaian ke atas data lebih mudah. Jabatan Akauntan Negara Malaysia (JANM) menggunakan beberapa jenis pangkalan data oleh pelbagai kategori pengguna bagi memenuhi kehendak dan keperluan maklumat di dalam jabatan. Setiap pangkalan data dikendalikan oleh pentadbir pangkalan data masing-masing.

## 2.0 OBJEKTIF

Tujuan garis panduan pengurusan pangkalan data adalah untuk:

(a) Menerangkan dengan lebih terperinci tatacara penggunaan dan pengurusan pangkalan data kepada semua warga JANM;

(b) Memastikan pangkalan data digunakan dengan betul dan selamat; dan

(c) Meminimakan sebarang permasalahan berkaitan pangkalan data.

## 3.0 SKOP

Prosedur ini menerangkan tatacara penggunaan dan pengurusan pangkalan data di JANM.

## 4.0 BIDANG DKICT

Bidang yang dirujuk adalah seperti berikut:

(a) Bidang 5 : Keselamatan Fizikal Dan Persekitaran

- 050203 Media Storan
- 050208 Pelupusan Perkakasan / Media Elektronik

(b) Bidang 6 : Pengurusan Operasi Dan Komunikasi

- 060302 Penerimaan Sistem
- 060501 *Backup*
- 060502 *Housekeeping* Storan
- 060503 Pengorganisasian semula *(Reorganisation)*
- 060701 Penghantaran dan Pemindahan
- 060702 Prosedur Pengendalian Media
- 061003 Sistem Log
- 061004 Pemantauan Log

(c) Bidang 7 : Kawalan Capaian

- 070201 Akaun Pengguna
- 070202 Hak Capaian
- 070601 Capaian Aplikasi dan Maklumat

(d) Bidang 8 : Perolehan, Pembangunan Dan Penyelenggaraan Sistem

- 080101 Keperluan Keselamatan Sistem Maklumat
- 080301 Kawalan Sistem Fail
- 080401 Prosedur Kawalan Perubahan

## 5.0 PEMAKAIAN

Pemakaian garis panduan ini meliputi:

a) Pemilik Sistem
b) Pentadbir Pangkalan Data
c) Pengguna Pangkalan Data

## 6.0 PENGECUALIAN

Prosedur ini terpakai untuk semua pihak seperti di para 5.0 kecuali telah mendapat kebenaran bertulis daripada CIO.

## 7.0 PENGURUSAN DAN PENGENDALIAN

| No. | Perkara | Peranan |
|---|---|---|
| 7.1 Peranan Dan Tanggungjawab | | |
| a. | Pemilik Sistem<br>Pemilik Sistem merupakan pemilik kepada semua sistem aplikasi yang ada di Jabatan Akauntan Negara Malaysia. | Pemilik |
| b. | Pentadbir Pangkalan Data<br>Pentadbir Pangkalan data adalah bertanggungjawab:<br>i. Bertanggungjawab untuk menyediakan, menyelenggara dan menaik taraf terhadap semua pangkalan data *Production* dan *Non-Production*;<br>ii. Memastikan Keselamatan dalam menguruskan kebenaran capaian pangkalan data dipatuhi;<br>iii. Mendokumenkan maklumat kebenaran capaian terhadap pangkalan data;<br>iv. Menetapkan tempoh simpanan maklumat permohonan akses kebenaran terhadap pangkalan data;<br>v. Memantau dan merancang keperluan kapasiti untuk pangkalan data.<br>vi. Menjalankan, memantau dan menyenggara *backup* sistem JANM di semua lokasi JANM mengikut jadual yang ditetapkan;<br>vii. Melaksanakan *backup* secara manual sekiranya *backup* yang telah dijadualkan tidak berjaya;<br>viii. Memastikan setiap salinan *backup* bagi setiap sistem berjaya dan boleh digunakan bagi aktiviti pemulihan (*restore*) sistem jika diperlukan; dan<br>ix. Menjalankan aktiviti simulasi pemulihan sistem (*restore and recovery*) secara berkala dengan menggunakan salinan *backup* bagi membolehkan sistem digunakan semula. | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| c. | Pengguna Pangkalan Data<br>i. Definisi pengguna – memberi hak capaian pangkalan data yang ditetapkan melalui antaramuka yang disediakan | Pengguna |
| 7.2 Keselamatan Fizikal Dan Persekitaran | | |
| a. | Media Storan<br>Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.<br>i. Perkara-perkara yang perlu dipatuhi bagi penyimpanan media storan adalah seperti berikut:<br>(a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;<br>(b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;<br>(c) Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan;<br>(d) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;<br>(e) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data dan disimpan mengikut prosedur *backup* yang telah ditetapkan;<br>(f) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat mengikut prosedur pelupusan; dan | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| | (g) Penghapusan maklumat atau kandungan media storan mestilah mendapat kelulusan pemilik maklumat terlebih dahulu. | |
| b. | Pelupusan Perkakasan dan media storan<br><br>Semua peralatan ICT termasuk media storan yang telah rosak, usang dan tidak ekonomi untuk dibaiki sama ada harta modal atau inventori hendaklah dilupuskan mengikut prosedur pelupusan yang ditetapkan.<br><br>Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan JANM.<br><br>i. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;<br>(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;<br>(c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;<br>(d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| | (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br>(f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; dan<br>(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa. | |
| 7.3 Penyelenggaraan Pangkalan Data | | |
| | Pengorganisasian semula (*Re-org*) dilakukan bagi menyusun semula ruangan pangkalan data manakala proses *housekeeping* dijalankan bagi memastikan ruang storan digunakan secara optimum.<br>Pengemaskinian patches perlu dilakukan bagi memastikan sistem berada dalam standard terkini yang bersesuaian dan menepati keperluan sistem aplikasi dan pangkalan data. | Pentadbir |
| 7.4 Backup & Restore | | |
| | *Backup* hendaklah dilakukan secara berjadual atau setiap kali konfigurasi berubah bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana atau berdasarkan keperluan.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>i. Melaksanakan *backup* ke atas semua sistem perisian, aplikasi dan pangkalan data termasuk log mengikut keperluan;<br>ii. *Backup* hendaklah dilakukan di dalam media yang bersesuaian; | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| | iii. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat mengikut polisi yang ditetapkan.<br>iv. Menyimpan generasi *backup* mengikut prosedur *backup* yang telah ditetapkan oleh jabatan; dan<br>v. Menguji secara berkala aktiviti *restore* bagi memastikan sistem berjaya digunakan dan dapat berfungsi dengan sempurna. | |
| 7.5 Kawalan Capaian | | |
| | Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>i. Setiap pengguna diberikan hak capaian mengikut had capaian<br>ii. Data-data dari production tidak dibenarkan menggunakan bagi tujuan pengujian<br>iii. Mendokumenkan maklumat kebenaran capaian terhadap pangkalan data.<br>iv. Menetapkan tempoh simpanan maklumat permohonan akses kebenaran terhadap pangkalan data.<br>v. Pemilihan, penggunaan, penukaran dan pengurusan kata laluan bagi mencapai sistem ICT seperti di bidang 7 dokumen DKICT versi 5.1.<br>vi. Pemantauan berkala terhadap kebenaran capaian pangkalan data. | Pentadbir |
| 7.6 Kawalan Perubahan | | |
| | Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br>i. Perubahan dan/atau pindaan ke atas pangkalan data perlu dikawal, diuji, direkodkan, disahkan sebelum diguna pakai dan dihadkan mengikut keperluan;<br>ii. Sebarang peluang untuk membocorkan maklumat perlu dihalang. | Pentadbir |

# BAB 5 - PENGURUSAN KESELAMATAN SISTEM APLIKASI TERAS

## 1.0 PENGENALAN

Sistem aplikasi teras Jabatan Akauntan Negara Malaysia (JANM) adalah sistem yang melibatkan pengurusan perakaunan dan kewangan di JANM.

## 2.0 OBJEKTIF

Objektif prosedur keselamatan sistem aplikasi ini adalah:

a) Memastikan kelancaran operasi sistem dengan meminimumkan risiko keselamatan berkaitan dengan sistem aplikasi teras JANM
b) Memberi panduan dan rujukan bagi memastikan capaian kepada persekitaran pembangunan aplikasi teras adalah selamat dan terkawal

## 3.0 SKOP

Prosedur ini menerangkan tatacara perolehan, pembangunan dan panduan keselamatan bagi pemilik sistem, pentadbir sistem, pegawai teknikal, pentadbir pengguna sistem, pihak ketiga dan pengguna yang menggunakan sistem aplikasi teras di JANM.

## 4.0 BIDANG DKICT

Bidang Dasar Keselamatan ICT yang berkaitan dengan prosedur keselamatan sistem aplikasi teras adalah seperti berikut:

a) Bidang 7: Kawalan Capaian
    - 070101 keperluan kawalan capaian
    - 070201 Akaun pengguna
    - 070203 pengurusan kata laluan
    - 070301 penggunaan kata laluan
    - 070601 capaian aplikasi dan maklumat

b) Bidang 8: Perolehan, Pembangunan dan Penyenggaraan Sistem
   - 080102 pengesahan Data Input dan Output

c) Bidang 9 - Pengurusan Pengendalian Insiden Keselamatan
   - 080102 pengesahan Data Input dan Output

## 5.0 PEMAKAIAN

Pemakaian prosedur keselamatan ini meliputi:

1) Pemilik sistem
2) Pentadbir sistem
3) Pegawai teknikal
4) Pentadbir pengguna sistem
5) Pengguna sistem
6) Pihak ketiga

## 6.0 PENGECUALIAN

Prosedur ini terpakai kepada pemilik sistem, pentadbir sistem, pegawai teknikal, pentadbir pengguna sistem, pengguna sistem dan pihak ketiga sistem aplikasi teras JANM kecuali dengan kebenaran bertulis daripada ICTSO.

## 7.0 PENGURUSAN DAN PENGENDALIAN

| No. | Perkara | Peranan |
|---|---|---|
| 7.1 Perolehan Sistem | | |
| a. | Perolehan untuk sistem aplikasi hendaklah berdasarkan kepada Pelan Strategik ICT (ISP) Jabatan dengan mematuhi panduan keselamatan aplikasi ISP serta mengikut pekeliling semasa yang berkuat kuasa. | Pemilik Sistem |

| No. | Perkara | Peranan |
|---|---|---|
| b. | Kajian pasaran seperti kesesuaian teknologi dan ciri-ciri keselamatan yang perlu ada bagi sistem aplikasi hendaklah dilaksanakan berasaskan keperluan sebenar yang dikenal pasti bagi tujuan sebarang perolehan sistem teras JANM. | Pemilik Sistem |
| 7.2 Pembangunan Sistem | | |
| a. | Pembangunan sistem aplikasi hendaklah berpandukan kepada *System Development Life Cycle* (SDLC) yang terdiri daripada beberapa fasa seperti *Planning, Requirement Analysis, Design, Development, Integration* dan *Testing*. | Pemilik & Pentadbir Sistem |
| b. | Data input perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian seperti berikut:<br>*Constrain input* - menentukan apa yang dibenarkan pada *field*<br>*Validate data- type*, *length*, format dan *range*<br>*Reject known bad input* - tidak menerima data yang berkemungkinan *malicious.* | Pemilik & Pentadbir Sistem |
| c. | Pembangunan sistem aplikasi hendaklah menguji fungsian dan *performance* sistem berdasarkan persekitaran sebenar. | Pemilik & Pentadbir Sistem |
| d. | Pengujian sistem yang dilaksanakan hendaklah sehingga ke peringkat *Final Acceptance Test* (FAT). | Pemilik & Pentadbir Sistem |
| e. | Pengujian sistem hendaklah dilaksanakan di dua persekitaran yang berlainan iaitu pengujian persekitaran *Development* sebelum dilaksanakan di persekitaran *Production*. | Pemilik & Pentadbir Sistem |
| f. | Mesej ralat tidak boleh memaparkan mesej dalaman sistem seperti nama *table*, prosedur, *error code* dan sebagainya kepada pengguna bagi mengelak risiko digodam. | Pentadbir sistem |

| No. | Perkara | Peranan |
|---|---|---|
| g. | URL *query string* tidak boleh memaparkan sebarang maklumat *session* pengguna seperti: *https://www.example.net/servlet/login?userid=abu&password=abu* | Pentadbir sistem |
| 7.3 Penyenggaraan Sistem | | |
| a | Pemindahan teknologi dan pengetahuan hendaklah dilaksanakan dengan sempurna dalam tempoh kontrak bagi memastikan pegawai teknikal jabatan berupaya menyenggara sistem aplikasi selepas tamat tempoh jaminan. | Pemilik, Pentadbir sistem & Pihak Ketiga |
| b. | Penyenggaraan sistem hanya boleh dilakukan oleh kakitangan atau pihak yang dibenarkan sahaja. Semua aktiviti penyenggaraan hendaklah disemak dan diuji sebelum dan selepas aktiviti tersebut dilaksanakan. | Pentadbir sistem & Pegawai Teknikal |
| c. | Sebarang penyenggaraan yang memerlukan sistem ditutup (*shutdown*) dan tidak boleh dicapai dalam tempoh tertentu perlu dirancang dan dimaklumkan kepada pengguna. | Pentadbir Sistem, Pegawai Teknikal & Pihak Ketiga |
| d. | Menyelesaikan masalah teknikal sistem aplikasi teras di peringkat sokongan pertama (*first level support*) dan melaporkan sebarang masalah berkaitan sistem aplikasi ke pihak yang bertanggungjawab berdasarkan Bidang 09 Pengurusan Pengendalian Insiden Keselamatan DKICT. | Pegawai Teknikal |
| e. | Perjanjian Tahap Perkhidmatan (*Service Level Agreement*) perlu wujud antara JANM dengan pembekal sistem aplikasi agar | Pemilik Sistem dan |

| No. | Perkara | Peranan |
|---|---|---|
| | sebarang kerosakan pada perkakasan sistem tersebut dapat dipulihkan dalam tempoh 24 jam. | Pihak Ketiga |
| f. | Penyenggaraan mencegah oleh pihak pembekal hendaklah dilakukan secara berkala bagi memastikan sistem aplikasi dapat beroperasi dengan lancar. | Pentadbir Sistem dan Pihak Ketiga |
| 7.4 Source code | | |
| a. | *Source Code* dan/atau *Intellectual Property Rights* (IPR) bagi pembangunan sistem aplikasi dan serahan-serahan lain yang berkaitan hendaklah menjadi Hak Milik JANM. | Pemilik Sistem |
| b. | Sebarang aktiviti yang melibatkan penambahbaikan pada *source code* sedia ada disebabkan oleh *system bugs* perlu mengisi borang yang telah ditetapkan contoh *Observation Report* (OR) dan mendapat kebenaran daripada pentadbir sistem. | Pentadbir Sistem dan Pihak Ketiga |
| c. | Sekiranya terdapat penambahbaikan yang baru pada sistem aplikasi yang melibatkan perubahan pada *source code* perlu mengisi borang yang telah ditetapkan oleh pemilik sistem contoh Borang *Change Request* (CR). | Pentadbir Sistem dan Pihak Ketiga |
| d | Mengenalpasti tahap keselamatan aplikasi dengan menganalisa *source code*.Ia adalah proses verifikasi samada aplikasi tersebut telah mempunyai kawalan keselamatan yang mencukupi dan berfungsi dengan betul. *Secure Code review* adalah satu cara memastikan aplikasi yang telah dibangunkan terjamin tahap keselamatannya. | Pentadbir Sistem dan Pihak Ketiga |

| No. | Perkara | Peranan |
|---|---|---|
| 7.5 Authentication | | |
| a. | Bagi menghalang id pengguna dan kata laluan daripada digodam, kata laluan hendaklah dikunci selepas beberapa kali percubaan. Akaun tersebut hendaklah dikunci untuk tempoh masa yang tertentu bagi mengelakkan akaun terus digodam. | Pentadbir & Pengguna sistem |
| b. | Penetapan kata laluan hendaklah merujuk kepada DKICT Bidang 07 Kawalan Capaian: Pengurusan Kata Laluan. | Pengguna Sistem |
| c. | *Default* akaun dan *default password* tidak boleh diguna pakai dan hendaklah dinamakan semula kepada nama yang bersesuaian dan selamat. | Pentadbir & Pengguna sistem |
| d. | Kata laluan baru hendaklah diwujudkan setiap kali pengguna lupa kata laluan dan pengguna perlu memberikan PUK/SOPIN bagi sistem yang mengguna pakai token /kad pintar. | Pentadbir & Pengguna sistem |
| e. | Kata laluan hendaklah di *hash* (*one-way-hash*) apabila disimpan di dalam pangkalan data. | Pentadbir sistem |
| 7.6 Authorization and Access Control | | |
| a. | Sistem hendaklah berupaya menghalang pengguna daripada akses kepada sistem melalui *page* yang tidak dibenarkan dengan menggunakan *file path* pada URL. | Pentadbir sistem |
| b. | Sistem perlu berupaya untuk memastikan *back arrow* tidak berfungsi untuk kembali ke halaman sebelumnya. | Pentadbir sistem |

| No. | Perkara | Peranan |
|---|---|---|
| 7.7 Authorization dan Access Control – rujuk Prosedur Pengurusan Pangkalan Data (Backup & Restore) | | |
| 7.8 Integrasi dengan Sistem Luar | | |
| a. | *Interface Description Document* (IDD) hendaklah lengkap dengan format seperti *source*, *destination, size data, type, field*, *message code, message description* dan *field delimiter* serta mempunyai mekanisme bagi pengurusan ralat dan pengesahan penghantaran/penerimaan data/mesej. | Pentadbir Sistem |

## BAB 6 - PENGURUSAN KESELAMATAN SISTEM APLIKASI SOKONGAN

### 1.0 PENGENALAN

Aplikasi sokongan di JANM adalah selain daripada aplikasi teras yang dibangunkan untuk menyokong keperluan-keperluan lain Jabatan. Aplikasi tersebut adalah terdiri dari Knowledge Management, Intranet, Laman Web Akruan, AGHR, Sistem Self Assessment Nilai, eCPS, eKursus, Buletin GFMAS, Sistem Pengurusan Aset, Sistem ePenyata Gaji & Laporan (eSPGL), eMaklum dan lain-lain. Prosedur ini **mestilah** dirujuk bersama dengan Dasar Keselamatan ICT Jabatan Akauntan Negara Malaysia (DKICT JANM).

### 2.0 OBJEKTIF

Tujuan prosedur ini adalah untuk:

i. Memberi panduan kepada pemilik, Pentadbir Sistem ICT dan penyelaras aplikasi dari aspek keselamatan dalam menyelia dan mengurus aplikasi sokongan di JANM sama ada yang akan dibangunkan secara dalaman (*in-house*) atau sumber luar (*outsource*) dan juga aplikasi sokongan sedia ada bagi mematuhi Dasar Keselamatan ICT (DKICT) JANM.

ii. Memastikan aplikasi sokongan yang dibangunkan untuk capaian awam *(public access)* mematuhi kriteria yang ditetapkan di dalam penilaian *Provider-Based Evaluation* (ProBE) oleh pihak MAMPU.

iii. Memastikan data dan maklumat sistem aplikasi dilindungi bagi menjamin integriti;

### 3.0 SKOP

Prosedur ini menerangkan tatacara pembangunan, pengoperasian, penyenggaraan dan pemantauan di samping peraturan yang perlu diikuti untuk menjamin tahap keselamatan sistem-sistem aplikasi sokongan di JANM.

## 4.0 BIDANG DKICT

Bidang dirujuk adalah berikut:

(a) Bidang 02: Organisasi Keselamatan

- 0201 Infrastruktur Organisasi Dalaman
- 0202 Pihak Ketiga

(b) Bidang 04: Keselamatan Sumber Manusia

- 040103 Bertukar Atau Tamat Perkhidmatan

(c) Bidang 05: Keselamatan Fizikal dan Persekitaran

- 050205 Media Perisian dan Aplikasi

(d) Bidang 06: Pengurusan Operasi dan Komunikasi

- 060102 Kawalan Perubahan
- 060302 Penerimaan sistem
- 0605 *Housekeeping*
- 0609 Perkhidmatan Atas Talian/eDagang dan Maklumat Umum
- 0610 Pemantauan

(e) Bidang 07 Kawalan Capaian

(f) Bidang 08 Perolehan, Pembangunan Dan Penyenggaraan Sistem

## 5.0 PEMAKAIAN

Pemakaian prosedur ini meliputi:

a) Pemilik sistem aplikasi sokongan;

b) Pentadbir sistem aplikasi sokongan;

c) Penyelaras sistem aplikasi sokongan; dan

d) Pihak ketiga iaitu pihak luar yang menjalankan perkhidmatan dengan JANM.

## 6.0 PENGECUALIAN

Prosedur ini terpakai untuk semua pihak seperti di para 5.0 kecuali telah mendapat kebenaran bertulis daripada CIO.

## 7.0 PENGURUSAN DAN PENGENDALIAN

| No. | Perkara | Peranan |
|---|---|---|
| 7.1 Fasa Pra-Pembangunan | | |
| a. | Memastikan peruntukan mencukupi bagi pembangunan. | Pemilik |
| b. | Mendapatkan kelulusan untuk perolehan, bekalan dan/atau perkhidmatan daripada Jawatankuasa Pemandu ICT (JPICT). | Pemilik |
| c. | Perolehan hendaklah merujuk kepada Manual Prosedur Kerja dan lain-lain prosedur yang berkaitan. | Pemilik |
| d. | Pemilik memastikan aplikasi yang akan dibangunkan mendapat khidmat nasihat teknikal dari penyelaras melalui pengesahan Borang Senarai Semak Keperluan Aplikasi Sokongan JANM serta Borang Kawalan Perubahan sekiranya melibatkan *Change Request.* | Pemilik, Penyelaras |
| e. | Bertanggungjawab sepenuhnya (*ownership*) ke atas proses, data/maklumat sistem serta pengoperasian aplikasi. | Pemilik |
| f. | Memperjelas dan memahami keperluan terhadap pembangunan sistem. | Pemilik, Pentadbir |
| g. | Memastikan infrastruktur ICT yang diperlukan adalah mencukupi dan disenggara dengan baik. | Penyelaras |
| h. | Memastikan semua perisian adalah sah, berlesen dan sentiasa disenggara. | Pemilik, Penyelaras |

| No. | Perkara | Peranan |
|---|---|---|
| i. | Menggunapakai piawaian perisian dengan patch terkini. Perisian yang disyorkan adalah seperti di **Jadual 1**. | Pentadbir |
| j. | Memastikan setiap *server* dipasang dengan *antivirus* mengikut kesesuaian. | Penyelaras |
| k. | Memastikan aplikasi mempunyai khidmat sokongan dan penyenggaraan. | Pemilik |
| l. | Bagi aplikasi atas talian untuk capaian awam, aplikasi hendaklah memenuhi kriteria yang ditetapkan di dalam penilaian *Provider-Based Evaluation* (ProBE) oleh pihak MAMPU seperti berikut:-<br>i. Notifikasi bagi setiap penamatan transaksi (*notification of transaction*);<br>ii. Panduan penggunaan aplikasi dan dipaparkan pada laman utama aplikasi;<br>iii. Memenuhi ciri-ciri keselamatan aplikasi atas talian;<br>iv. Mempunyai pelbagai bahasa iaitu sekurang-kurangnya Bahasa Malaysia dan Bahasa Inggeris. Penterjemahan kandungan ke dalam setiap bahasa perlu secara menyeluruh dan tidak menggunakan *auto translate;*<br>v. Statistik capaian pengguna; dan<br>vi. Rekabentuk responsif untuk paparan di peranti mudah alih (*responsive design*). | Pemilik, Pentadbir |
| 7.2 Fasa Pembangunan | | |
| a. | Menentukan dan mengesahkan peranan dan tahap capaian pengguna aplikasi. | Pemilik |
| b. | Membuat dan mengemaskini konfigurasi peranan dan tahap capaian pengguna aplikasi. | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| c. | Memastikan perlindungan ke atas data terperingkat menggunakan *Secure Sockets Layer (SSL), Secure Shell (SSH), Public Key Infrastructure (PKI)* atau *Encryption.* | Pentadbir |
| d. | Memastikan adanya *session termination (frontend/ backend).* | Pentadbir |
| e. | Memastikan aplikasi memenuhi keperluan IPV6 (*IPV6 compliance).* | Pentadbir |
| f. | Menyekat paparan *Directory Listing.* | Pentadbir |
| g. | Mengkhususkan satu drive/volume/direktori secara berasingan untuk Sistem Pengoperasian, Pangkalan Data dan Aplikasi mengikut kesesuaian. | Pentadbir |
| h. | Memastikan dokumentasi sistem, prosedur operasi sistem (*Standard Operating Procedure - SOP),* dan manual panduan pengguna yang lengkap serta terkini. | Pemilik, Pentadbir |
| i. | Menyediakan khidmat nasihat ICT berkaitan pembangunan dan penyenggaraan aplikasi sokongan. | Penyelaras |
| j. | Memastikan ketersediaan sistem dengan menyediakan persekitaran *High Availability* (jika berkaitan). | Penyelaras |
| k. | Memastikan dengan jelas kriteria dan keperluan bagi penerimaan sistem, didokumenkan dan diuji sebelum sistem diterima. | Pemilik, Pentadbir |
| l. | Membuat konfigurasi dan pelarasan terhadap sistem pengoperasian, perisian pembangunan sistem dan pangkalan data untuk memberi perlindungan kepada aplikasi yang akan digunakan supaya keselamatan dan prestasi aplikasi di tahap yang optimum. | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| m. | Untuk mengelak daripada SQL Injection, operasi *SELECT, UPDATE, DELETE* dan *INSERT* keatas pangkalan data perlu dilakukan melalui *Stored Procedure*. | Pentadbir |
| n. | Maklumat katalaluan pengguna disimpan dalam bentuk *encrypted* di dalam pangkalan data. | Pentadbir |
| o. | Pembangunan aplikasi perlu berdasarkan Standard Terbuka untuk memastikan interoperabiliti dan aksesibiliti. | Pentadbir |
| p. | Aplikasi yang akan dibangunkan perlu mengambil kira kepelbagaian saluran elektronik (yang berkos efektif), di mana sesuai, bagi memastikan aksesibiliti pelanggan. | Pentadbir |
| q. | Borang elektronik (eForm) yang terdapat dalam aplikasi mestilah membenarkan pengguna membuat pembetulan dan mendapatkan pengesahan sebelum borang dihantar. (Contoh: sistem perlu memaparkan kotak dialog memohon pengesahan sebelum borang dihantar). | Pentadbir |
| r. | Sistem aplikasi mesti berupaya menyemak data yang dimasukkan bagi memastikan betul dan sesuai. Semakan input mesti dilaksanakan bagi mengesan kesilapan berikut di mana bersesuaian, sebagai contoh:<br>i. nilai di luar julat;<br>ii. data hilang atau tidak lengkap;<br>iii. aksara yang tidak sah dalam medan data;<br>iv. melebihi had;<br>v. *unauthorised data* (contoh: medan bagi kelulusan permohonan hanya boleh dikemas kini oleh personel yang diberi kuasa); dan<br>vi. Data tidak konsisten. | Pentadbir |
| s. | Memastikan aplikasi mempunyai jejak audit (audit trail) dan fail log bagi server dan aplikasi diaktifkan. | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| t. | Melaksanakan aktiviti pengukuhan **sebelum *Go Live*** aplikasi;<br>i. Mengukuhkan kata laluan server, pangkalan data, aplikasi dan lain-lain;<br>ii. Memastikan imbasan *Security Posture Assessment* (SPA) dibuat untuk menilai tahap keselamatan aplikasi, pelayan dan rangkaian;<br>iii. Melaksanakan pengukuhan hasil dari penemuan imbasan termasuk *patches*, *firmware* dan lain-lain; dan<br>iv. Memeriksa *Default Configuration serta* mengemaskini dan *disable* perisian/*services* yang tidak berkaitan; | Pentadbir |
| u. | Melakukan pengujian iaitu *functional*, *non-functional* dan *performance testing* untuk *validate* dan *verify* aplikasi yang dibangunkan memenuhi keperluan dan rekabentuk aplikasi. | Pemilik, Pentadbir |
| v. | Mengenalpasti tahap keselamatan aplikasi dengan menganalisa *source code*. Ia adalah proses verifikasi samada aplikasi tersebut telah mempunyai kawalan keselamatan yang mencukupi dan berfungsi dengan betul. *Secure Code review* adalah satu cara memastikan aplikasi yang telah dibangunkan terjamin tahap keselamatannya. | Pemilik, Pentadbir |
| 7.3 Fasa Pengoperasian, Penyenggaraan dan Pemantauan | | |
| a. | Memastikan aplikasi mempunyai khidmat sokongan dan penyenggaraan. | Pemilik |
| b. | Memastikan data dan maklumat dibawah pengurusannya sentiasa tepat, lengkap, kemas kini dan dilindungi bagi menjamin integriti. Ia hanya boleh diubah dengan cara yang dibenarkan. | Pemilik |

| No. | Perkara | Peranan |
|---|---|---|
| c. | Menyelaras khidmat bantuan teknikal kepada pengguna yang menghadapi masalah aplikasi. | Penyelaras |
| d. | Mengemaskini Manual Proses Kerja selaras dengan proses sistem baharu. | Pemilik |
| e. | Bertanggungjawab sepenuhnya (*ownership*) ke atas kesediaan aplikasi serta memantau penggunaannya. | Pemilik |
| f. | Memastikan dokumentasi aplikasi, prosedur operasi aplikasi (*Standard Operating Procedure - SOP*) dan manual panduan pengguna yang lengkap serta terkini. | Pemilik |
| g. | Membuat pengujian ke atas data selepas aktiviti *restore* dilakukan. | Pemilik, Pentadbir |
| h. | Memastikan dan memantau aplikasi boleh dicapai dan digunakan pada setiap masa. | Pemilik Pentadbir |
| i. | Melaksanakan aktiviti pengukuhan **semasa *Go Live*** aplikasi.<br>i. Melakukan pengauditan infrastruktur dan keselamatan ICT;<br>ii. Memastikan aktiviti imbasan vulnerabilities system (Aplikasi Pengoperasian, Pangkalan Data, Aplikasi dan Perisian) dilakukan secara berkala;<br>iii. Melaksanakan tindakan pengukuhan ke atas hasil penemuan *Security Posture Assessment* (SPA) mengikut keperluan;<br>iv. Mengemaskini *patches* sistem secara berterusan; dan<br>v. Melakukan peningkatan (*upgrade*) perisian / *firmware* mengikut keperluan | Penyelaras, Pentadbir |
| j. | Memastikan aplikasi disenggara mengikut jadual yang ditetapkan. | Pemilik |

| No. | Perkara | Peranan |
|---|---|---|
| k. | Memastikan setiap masalah aplikasi diselesaikan di dalam tempoh *Service Level Agreement* (SLA) yang ditetapkan di dalam kontrak. | Pemilik |
| l. | Bagi sebarang perubahan aplikasi yang dibuat hendaklah dipohon menggunakan Borang Kawalan Perubahan JANM seperti di Lampiran 4: Borang *Change Request.* | Pemilik |
| m. | Pengujian aplikasi perlu dilakukan apabila terdapat<br>i. perubahan sistem;<br>ii. perubahan perisian; atau<br>iii. perubahan perkakasan. | Pemilik,<br>Pentadbir |
| 7.4 Backup & Restore System Configuration dan Data | | |
| a. | Memantau dan memastikan salinan (*backup*) sistem dan pangkalan data pada server dibuat dan disimpan dengan selamat. | Pemilik,<br>Penyelaras |
| b. | Memastikan pemulihan *(recovery)* dan pemuliharaan *(conservation)* dilaksanakan. | Penyelaras |
| c. | Melakukan pengujian sistem setiap kali selepas proses pemulihan dan pemuliharaan dijalankan. | Pemilik,<br>Pentadbir |
| 7.5 Ciri-ciri Keselamatan Aplikasi | | |
| | Ciri-ciri keselamatan bagi aplikasi mengikut kesesuaian sistem adalah seperti berikut:<br>a. Logoff secara automatik apabila tiada aktiviti dalam tempoh tidak melebihi 30 minit atau mengikut sensitiviti data; | Pentadbir |

| No. | Perkara | Peranan |
|---|---|---|
| | b. Batalkan dengan segera semua hak capaian pengguna yang telah bertukar tugas, berpindah atau berhenti sebaik mendapat makluman dari pemilik.<br><br>c. Wujud pengenalan pengguna yang unik dalam sistem;<br><br>d. Sistem berupaya menggantung/menamatkan hak capaian pengguna yang tidak aktif selepas satu tempoh tertentu.<br><br>e. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;<br><br>f. Kuatkuasakan pertukaran kata laluan selepas 90 hari atau selepas suatu tempoh masa bersesuaian<br><br>g. Tidak membenarkan penggunaan semula kata laluan yang terakhir digunakan;<br><br>h. Server pangkalan data tidak dibenarkan diakses dari luar. Pengguna dalaman yang mengakses server pangkalan data perlu disahkan melalui pemetaan kepada Active Directory.<br><br>i. Sistem pengoperasian bagi aplikasi kritikal hendaklah menggunakan versi yang menyokong agen MyGSOC bagi tujuan pemantauan. | |
| 7.6 Kawalan Capaian | | |
| a. | Semua akses kepada aset ICT ditentukan dan didokumenkan melalui prosedur pendaftaran pengguna dan dikawal berdasarkan kepada:<br>i. prinsip perlu mengetahui;<br>ii. peranan;<br>iii. hak akses minimum; dan<br>iv. Pengasingan tugas. | Penyelaras |

| No. | Perkara | Peranan |
|---|---|---|
| b. | Semua hak keistimewaan dan akses hendaklah dikaji semula secara berkala. Akses yang mempunyai hak keistimewaan hendaklah dihadkan dan dipantau setiap hari. | Penyelaras |
| c. | Tahap capaian perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. | Penyelaras |
| d. | Mendapat capaian ke sistem-sistem di JANM dengan mengisi seperti di Lampiran 1 : Borang Pendaftaran Kawalan Akses ICT, Jabatan Akauntan Negara Malaysia (JANM). | Semua |
| e. | Memaklumkan Pentadbir Sistem ICT Rangkaian & Keselamatan sekiranya tidak memerlukan akaun bagi tujuan capaian lagi dengan mengisi borang seperti di Lampiran 2 : Borang Penamatan Perkhidmatan Kawalan Akses ICT | Semua |
| f. | Aktiviti akses dipantau untuk mengesan aktiviti luar biasa seperti cubaan berulang akses yang tidak sah yang mungkin mengancam integriti, kerahsiaan atau ketersediaan sistem. (F5, GSOC). | Penyelaras |
| g. | Setiap pengguna dikenal pasti dengan pengenalan identiti pengguna yang unik dan hendaklah disahkan sebelum mendapat akses kepada sumber maklumat. | Pentadbir Sistem ICT |
| h. | Maklumat pengenalan identiti, kata laluan dan pengesahan hendaklah dirahsiakan. | Semua |

## 9.0 PIHAK KETIGA

a) Pengguna dan Pembekal/kontraktor penyenggaraan yang memerlukan akaun bagi mendapat capaian ke sistem-sistem di JANM perlu mengisi Borang Pendaftaran Kawalan Akses ICT, JANM seperti di Lampiran 1 : Borang Pendaftaran Kawalan Akses ICT, Jabatan Akauntan Negara Malaysia (JANM).

b) Pengguna dan Pembekal/kontraktor penyenggaraan bertanggungjawab untuk memaklumkan kepada Penyelaras sekiranya tidak memerlukan

akaun bagi tujuan capaian lagi dengan mengisi Borang Penamatan Perkhidmatan Kawalan Akses ICT, JANM seperti di Lampiran 2 : Borang Penamatan Perkhidmatan Kawalan Akses ICT.

c) Pentadbir Sistem ICT bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga.

**Jadual 1**

**Piawaian Perisian**

| Keperluan Teknikal | Jenis Perisian |
|---|---|
| Sistem Pengoperasian | 1. Windows<br>2. Linux |
| Pangkalan Data | 1. Microsoft SQL<br>2. MySQL<br>3. Microsoft Access |
| Bahasa Pengaturcaraan | 1. PHP<br>2. Java<br>3. HTML<br>4. XML<br>5. .Net |
| Web Server | 1. IIS<br>2. Apache<br>3. NGINX |
| *Content Management System (CMS)* | 1. Word Press<br>2. Joomla! |
| Multimedia Software | 1. Adobe Photoshop<br>2. Adobe Illustrator<br>3. Adobe Indesign<br>4. Final Cut Pro<br>5. Pinnacle |
| Development / Reporting Tools | 1. Adobe Dreamweaver<br>2. Notepad++<br>3. Crystal Report |
| Backup Software | 1. Symantec Netbackup |
| Browser | 1. Internet Explorer<br>2. Google Chrome<br>3. Mozilla Firefox<br>4. Safari |

# LAMPIRAN 1

## Borang Pendaftaran Kawalan Akses ICT

**BORANG PENDAFTARAN KAWALAN AKSES ICT**
**JABATAN AKAUNTAN NEGARA MALAYSIA (JANM)**

No. Rujukan: BPTM/SPICT/AKSES/A/<tahun – bil>

**Kepada: Pengarah Bahagian Pengurusan Teknologi Maklumat**

<table>
<tr><th>BIL</th><th>PERKARA</th><th>MAKLUMAT</th></tr>
<tr><td>1.</td><td>Nama Pemohon (Huruf Besar)</td><td></td></tr>
<tr><td>2.</td><td>Jawatan</td><td></td></tr>
<tr><td>3.</td><td>Nombor Kad Pengenalan / Passport</td><td></td></tr>
<tr><td>4.</td><td>Warganegara</td><td></td></tr>
<tr><td>5.</td><td>Alamat E-Mel</td><td></td></tr>
<tr><td>6.</td><td>No. Telefon</td><td></td></tr>
<tr><td>7.</td><td>Nama Organisasi</td><td></td></tr>
<tr><td>8.</td><td>Alamat Organisasi</td><td></td></tr>
<tr><td>9.</td><td>Nyatakan tahap dan justifikasi keperluan akses ke sistem-sistem tertentu di JANM (jika ada)<br>Lokasi Sistem:<br>☐ HO (Ibu Pejabat JANM<br>☐ PRD (I-City, Shah Alam)<br>☐ DRC (Petaling Jaya)<br>☐ Cawangan Lain (Nyatakan)<br>_____<br>_____<br>_____<br>_____<br>_____<br>_____<br>_____<br>_____</td><td>
<table>
<tr><th>Nama Sistem</th><th>Tahap dan Tujuan Akses</th></tr>
<tr><td>1. VPN<br>a) No. Siri PC<br>b) Alamat MAC</td><td>a) _____<br>b) _____<br>Tujuan:</td></tr>
<tr><td>2. Server:<br>a)_____<br>b)_____</td><td>a) _____<br>b) _____</td></tr>
<tr><td>3. Sistem:<br>a)_____<br>b)_____</td><td>a) _____<br>b) _____</td></tr>
<tr><td>4. Lain-Lain:<br>a)_____<br>b)_____</td><td>a) _____<br>b) _____</td></tr>
</table>
</td></tr>
</table>

**Pengakuan Pemohon:**
Saya akan mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan Malaysia. Saya juga akan memaklumkan kepada pihak Bahagian Pengurusan Teknologi Maklumat, JANM mengenai penamatan perkhidmatan saya sebagai kakitangan organisasi yang tersebut di atas atau apabila kontrak organisasi dengan JANM tamat dengan mengisi dan menghantar Borang Penamatan Kawalan Akses ICT.

| **Tandatangan Pemohon & Cop Rasmi**<br>**Organisasi:**<br><br>.....<br><br>Tarikh: | **Pengesahan Ketua Unit/Seksyen & Cop Rasmi:**<br><br><br>.....<br><br>Tarikh: |
|---|---|

**Maklumat Permohonan:Untuk Kegunaan BPTM Sahaja**

Sukacita dimaklumkan bahawa permohonan anda telah diluluskan/*tidak diluluskan.

Berikut adalah maklumat akaun sementara anda:

| **Nama Sistem** | **Pengesahan Pentadbir Sistem** | | **ID/*Username*** | **Kata Laluan** |
|---|---|---|---|---|
| | **Nama** | **Tandatangan** | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Sebarang pertanyaan hendaklah berurusan terus dengan:
Unit Rangkaian dan Keselamatan, SPICT,
Aras 5, Bahagian Pengurusan Teknologi Maklumat,
Kompleks Kementerian Kewangan,
No. 1, Persiaran Perdana, Precint 2,
62594 Putrajaya.

Tel : 03-8882 1232 / 03-8882 1266
Emel : networksecurity@anm.gov.my
Catatan :

# LAMPIRAN 2

## Borang Penamatan Perkhidmatan Kawalan Akses ICT

**BORANG PENAMATAN PERKHIDMATAN KAWALAN AKSES ICT**
**JABATAN AKAUNTAN NEGARA MALAYSIA (JANM)**

No. Rujukan: BPTM/SPICT/AKSES/B/<tahun-bil>

**Kepada: Pengarah Bahagian Pengurusan Teknologi Maklumat**

| BIL | PERKARA | MAKLUMAT |
|---|---|---|
| 1. | Nama Pemohon (Huruf Besar) | |
| 2. | Jawatan | |
| 3. | Nombor Kad Pengenalan / Passport | |
| 4. | Warganegara | |
| 5. | Alamat E-Mel | |
| 6. | No. Telefon | |
| 7. | Nama Organisasi | |
| 8. | Alamat Organisasi | |
| 9. | Sebab-Sebab Penamatan | ☐ 9.1 Tugas di JANM selesai / ditamatkan oleh syarikat pembekal / Organisasi / JANM<br>☐ 9.2 Bersara / Tamat Perkhidmatan di syarikat pembekal / Organisasi / JANM<br>☐ 9.3 Melanggar prosedur penggunaan tempat / sistem di JANM (sila nyatakan)<br>……<br>☐ 9.4 Lain-lain (sila nyatakan)<br>…… |

**Nota:**
Bagi perkara 9.3, borang ini perlulah ditandatangani oleh Timbalan Pengarah Seksyen Perkhidmatan ICT BPTM.

Dengan ini adalah disahkan akaun pembekal berkenaan ditamatkan atas sebab-sebab di atas.

| **Tandatangan Wakil Organisasi:** | **Pengesahan Ketua Unit/Seksyen & Cop Rasmi:** |
|---|---|
| ……<br>Tarikh: | ……<br>Tarikh: |

**Maklumat Permohonan:**

**Maklumat Permohonan:Untuk Kegunaan BPTM Sahaja**

Sukacita dimaklumkan bahawa permohonan penamatan ini telah diambil tindakan.

Berikut adalah maklumat akaun sementara yang telah dipadamkan:

| **Nama Sistem** | **Pengesahan Pentadbir Sistem** | | **ID/*Username*** | **Tarikh Penamatan Akses** |
|---|---|---|---|---|
| | **Nama** | **Tandatangan** | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Sebarang pertanyaan hendaklah berurusan terus dengan:
Unit Rangkaian dan Keselamatan, SPICT,
Aras 5, Bahagian Pengurusan Teknologi Maklumat,
Kompleks Kementerian Kewangan,
No. 1, Persiaran Perdana, Precint 2,
62594 Putrajaya.

Tel : 03-8882 1232 / 03-8882 1266
Emel : networksecurity@anm.gov.my
Catatan :

# LAMPIRAN 3

## Borang Change Request

| JANM-BPTM-P1-XX | | C.R. No: |
|---|---|---|

# CHANGE REQUEST FORM

## REQUESTOR INFORMATION

Requestor Name : _____
Unit : _____
Date : _____

Email : _____
Tel. No. : _____

## CHANGE INFORMATION

Product/Application:
Module/Unit :

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Functional:** | **GL** | **FM** | **CO** | **AP** | **AR** | **CM** | **MM** | **HRPAY** | **G-ALMOS** | **G-UMIS** |
| | | | | | | | | | | |
| | **G-SMIS** | **G-LOMIS** | **TREASURY** | **AUTH** | **WM** | **ALE** | **BW** | **ABC** | | |
| | | | | | | | | | | |
| **Infra:** | **BASIS** | **BACKUP** | **NETWORK** | **SECURITY** | **SERVER** | **DATA CENTER** | **UAG** | **Others (please specify)** | | |
| | | | | | | | | | | |

| Service Desk Log No. : | Description of content/change: |
|---|---|
| | _____<br>_____<br>_____<br>_____ |

Source Client/System :

| *Dev* | *QAS* | *Staging* | *Pre-prod* | *Production/SID* |
|---|---|---|---|---|
| | | | | |

| | | | |
|---|---|---|---|
| HO | | LAB | |
| CUP | | LBG | |
| AGR | | MLK | |
| BTL | | MIR | |
| CUS | | MOI | |
| DEF | | MOT | |
| EDU | | NSB | |
| HLT | | PER | |
| JHR | | PHG | |
| JPM | | PNG | |
| KCH | | PRK | |
| KDH | | SDK | |
| KDN | | SGR | |
| KEL | | SIB | |
| KGU | | SRI | |
| KKI | | SRK | |
| KKR | | TAW | |
| KPT | | TRG | |

Target Client Systems :

| *QAS* | *Staging* | *Pre-prod* | *Production/SID* |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| HO | | LAB | |
| CUP | | LBG | |
| AGR | | MLK | |
| BTL | | MIR | |
| CUS | | MOI | |
| DEF | | MOT | |
| EDU | | NSB | |
| HLT | | PER | |
| JHR | | PHG | |
| JPM | | PNG | |
| KCH | | PRK | |
| KDH | | SDK | |
| KDN | | SGR | |
| KEL | | SIB | |
| KGU | | SRI | |
| KKI | | SRK | |
| KKR | | TAW | |
| KPT | | TRG | |

**TYPE OF CHANGE**

| Client-dependent: | | New: | | Fix: | | Client-independent: *(if no target clients)* | | New: | | Fix: | |
|---|---|---|---|---|---|---|---|---|---|---|---|

**EFFECT OF CHANGE**

| Change process step: | | Change system configuration: | | Others *(please specify):* | |
|---|---|---|---|---|---|
| Change screen fields: | | Change backup compatibility: | | _____<br>_____ | |

| Environment: | | | | | | Change effected *(date)*: | Test Result: | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| DEV | | Staging | | Prod | | | OK | | Not OK | |
| QAS | | Pre-prod | | | | | Reason: _____ | | | |

**APPROVAL**

| **Verified By:** | **By: Team Leader**<br><br>(Signature) | **Approved By:** | **By: Manager**<br><br>(Signature) |
|---|---|---|---|
| Name: | | Name: | |
| Date: | | Date: | |

**ACTION**

| **Verified By:** | **By: Team Leader**<br><br>(Signature) | **Approved By:** | **By: Manager**<br><br>(Signature) |
|---|---|---|---|
| Name: | | Name: | |
| Date: | | Date: | |

Comment/Error messages if any:

_____

_____

# LAMPIRAN 4

## Senarai Rujukan dan Peraturan

## SENARAI RUJUKAN DAN PERATURAN

1) Akta Arkib Negara 2003;

2) Dasar Keselamatan ICT Jabatan Akauntan Negara Malaysia (JANM);

3) Surat Pekeliling Perbendaharaan Bil 3 Tahun 2013 – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology (ICT)* Kerajaan;

4) Surat Pekeliling Perbendaharaan 1/2014 – Langkah Penjimatan Dalam Kerajaan (Had Nilai Pembelian Terus Bagi Bekalan dan Perkhidmatan);

5) Surat Pekeliling AM 1/2009 – Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan;

6) Pekeliling Am Bilangan 3 Tahun 2014 – Pelaksanaan Kumpulan Wang Amanah Pembangunan Projek ICT Sektor Awam (KWAICT)

7) Surat Arahan Ketua Pengarah MAMPU bertarikh 11 September 2009 : Garis Panduan Pembangunan Kandungan Sektor Awam;

8) Surat Arahan Ketua Pengarah MAMPU bertarikh 11 September 2009 : Garis Panduan Penyediaan Berita Online dan Penyiaran Berita Online di Laman Web/Portal Agensi-agensi Kerajaan;

9) Pekeliling Perbendaharaan (1PP) – Punca Kuasa, Prinsip dan Dasar Perolehan Kerajaan (PK 1/2013);

10) 1 Pekeliling Perbendaharaan (1PP) – Kaedah Perolehan Kerajaan (PK 2.2/2013);

11) 1 Pekeliling Perbendaharaan (1PP) – Tatacara Pengurusan Aset Alih Kerajaan - Pelupusan (PK 2.6/2013);

12) 1 Pekeliling Perbendaharaan (1PP) – Tatacara Pengurusan Aset Alih Kerajaan - Penyelenggaraan (PK 2.7/2013);

13) 1 Pekeliling Perbendaharaan (1PP) – Pentadbiran Kontrak Dalam Perolehan Kerajaan (PK 4/2013);

14) 1 Pekeliling Perbendaharaan (1PP) – Garis Panduan Permohonan Perolehan Secara Rundingan Terus (PK 7.13/2013);

15) Garis Panduan Pembangunan Aplikasi Sokongan JANM;

16) Pelan Strategik ICT (ISP) Jabatan Akauntan Negara Malaysia (JANM).