

**Compliance**

**SAGA**

***SELF-ASSESSMENT SAGA COMPLIANCE REVIEW* *AGENSI KECIL* - SASAR (K)**

**BAHAGIAN KHIDMAT PERUNDING**

**JABATAN AKAUNTAN NEGARA MALAYSIA**

**NAMA AGENSI : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**KEMENTERIAN /**

**SUK NEGERI : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\*\*UNTUK KEGUNAAN SEKRETARIAT PEMATUHAN SAGA SAHAJA\*\***

**TARIKH LAWATAN : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**SIRI LAWATAN : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**SKOR FUNGSIAN : \_\_\_\_\_\_\_/ 8 KRITERIA**

**SKOR TEKNIKAL : \_\_\_\_\_\_\_/ 7 KRITERIA**

**TOTAL SKOR : \_\_\_\_\_\_\_/ 15 KRITERIA**

**RATING:**

**BAIK (10 – 15 KRITERIA)**

**MEMUASKAN (5 – 9 KRITERIA)**

**TIDAK MEMUASKAN (< 5 KRITERIA)**

**MAKLUMAT AGENSI:**

|  |  |  |
| --- | --- | --- |
| Latar Belakang Agensi | : |  |
| Alamat Agensi | : |  |
| Pegawai Bertanggungjawab | : |  |
| No. Telefon/ Faksimili | : |  |
| Bilangan Pengguna Sistem Aplikasi | : |  |
| Bilangan *Concurrent User* | : |  |
| Bilangan Cawangan | : |  |
| Lokasi Cawangan | : |  |

**MAKLUMAT SISTEM APLIKASI:**

|  |  |  |
| --- | --- | --- |
| Nama Sistem Aplikasi & Versi Terkini | : |  |
| Tarikh Pembangunan Sistem Aplikasi | : |  |
| Tarikh Pelaksanaan Sistem Aplikasi | : |  |
| Pembekal/ Pembangun Sistem Aplikasi | : |  |
| Senarai Modul Dalam Sistem Aplikasi Perakaunan & Kewangan | : |  |
| Senarai Sistem Sokongan Yang Berintegrasi Dengan Sistem Aplikasi Perakaunan & Kewangan | : |  |
| Capaian Sistem Aplikasi (Client/ Web based) | : |  |
| PlatformSistem Pengoperasian (Operating System-Platform)/ Versi Bagi Aplikasi | : |  |
| PlatformSistem Pengoperasian (Operating System-Platform)/ Versi Bagi Pangkalan Data | : |  |
| Perisian Pembangunan Aplikasi/ Versi | : |  |
| Perisian Pembangunan Pangkalan Data/ Versi | : |  |
| Spesifikasi Server Aplikasi | : |  |
| Spesifikasi ServerPangkalan Data | : |  |
| Kapasiti Storan Server Bagi Aplikasi & Pangkalan Data | : |  |
| Penggunaan (utilisation) Server Terkini Bagi Aplikasi & Pangkalan Data | : |  |

Tandakan (√) pada ruangan **‘YA’** atau **‘TIDAK’** dan catatan/ ulasan boleh diisi di ruangan **‘CATATAN AGENSI’**.

| **BIL.** | **KRITERIA PEMATUHAN SAGA** | **YA** | **TIDAK** | **CATATAN AGENSI** | **DOKUMEN SOKONGAN** |
| --- | --- | --- | --- | --- | --- |
| **A. KRITERIA FUNGSIAN** | | | | | |
| **1.** | **Piawaian Perakaunan Yang Diterima Pakai**  Agensi mematuhi Piawaian Perakaunan Diterima Umum (General Accepted Accounting Principles - GAAP) | | | | |
| **(a)** | Adakah agensi menerima pakai piawaian perakaunan yang ditetapkan oleh Jabatan Akauntan Negara Malaysia (JANM) iaitu MPSAS? Sekiranya agensi tidak menggunakan MPSAS, perlu mendapatkan Surat Kelulusan Pengecualian MPSAS daripada JANM. |  |  |  | Penyata Kewangan Terkini Yang Telah Diaudit  Surat Kelulusan Pengecualian Pemakaian MPSAS (jika berkaitan) |
| **(b)** | Adakah peraturan yang berkuat kuasa diterima pakai dalam penyediaan penyata kewangan seperti Akta/ Arahan/ Polisi dan lain-lain? Nyatakan. |  |  |  | Salinan Akta/ Arahan/ Polisi Dalaman berkaitan Perakaunan dan Kewangan |
| **2.** | **Asas Perakaunan Akruan**  Agensi mengamalkan perakaunan akruan. | | | | |
| **(a)** | Adakah sistem aplikasi agensi menggunakan asas perakaunan akruan? |  |  |  | Penyata Kewangan Terkini Yang Telah Diaudit (**Dasar - dasar Perakaunan)** |
| **(b)** | Adakah titik pengiktirafan dan catatan bergu adalah tepat dan betul bagi akaun berikut:     1. Hasil (Titik Pengiktirafan : Tarikh invois/ bil agensi yang dikeluarkan **atau** Tunai diterima). 2. Belanja (Titik Pengiktirafan : Tarikh barang/ perkhidmatan diterima *- Goods Received Notes (GRN)/ Delivery Order (DO)* **atau** Tarikh invois/ bil).   Nota :   1. Hasil dan belanja diperakaunkan secara bulanan melalui pelarasan manual adalah dibenarkan. Contoh : Belanja Susutnilai, Faedah Simpanan Tetap dan Faedah Pinjaman Kakitangan 2. Hasil dan belanja yang diakrukan hanya pada hujung tahun TIDAK DITERIMA. |  |  |  | Paparan skrin catatan bergu pengiktirafan Hasil  Paparan skrin catatan bergu pengiktirafan Belanja  *Standard Operating Procedure* (SOP) bagi memperakaunkan transaksi yang tidak menggunakan modul sebagai contoh faedah, deposit, aset, susut nilai dan lain-lain. |
| **3.** | **Kod Carta Akaun Yang Fleksibel**  Agensi mempunyai Kod Carta Akaun merangkumi Aset, Liabiliti, Ekuiti, Hasil dan Belanja. | | | | |
| **(a)** | Adakah Kod Carta Akaun adalah fleksibel iaitu boleh ditambah/ dinyahaktif (deactivate) ? Nyatakan bilangan kelas Kod Carta Akaun.  Contoh: 4 Bilangan Kelas Kod Carta Akaun   |  |  |  |  | | --- | --- | --- | --- | | **Jenis Akaun** | **Kelas Akaun** | **Sub Kelas** | **Siri** | | **L**  (1 aksara) | **9**  (1 aksara) | **9**  (1 aksara) | **999**  (3 aksara) | |  |  |  | Salinan Kod Carta Akaun  Penerangan mengenai bilangan pecahan Kod Carta Akaun |
| **(b)** | Adakah Kod Carta Akaun diklasifikasi mengikut kategori aset, liabiliti, ekuiti, belanja dan hasil? |  |  |  | Salinan Kod Carta Akaun bagi setiap kategori L.E.B.A.H atau yang setara |
| **4.** | **Aliran Kerja Kelulusan Dokumen Kewangan**  Proses aliran kerja diamalkan dalam meluluskan dokumen kewangan. | | | | |
| **(a)** | Adakah proses aliran kerja diamalkan dalam meluluskan dokumen kewangan berikut:   1. Pesanan Tempatan? 2. Baucar Bayaran? 3. Baucar Jurnal?   Nyatakan bilangan proses aliran kerja bagi setiap dokumen kewangan tersebut.  Nota: Pegawai yang sama tidak dibenarkan menyemak dan melulus dokumen yang sama. |  |  |  | Paparan skrin proses sedia dan posting Pesanan Tempatan/ Baucar Bayaran/ Baucar Jurnal  *Standard Operating Procedure* (SOP) kelulusan dokumen kewangan |
| **(b)** | Adakah maklumat berikut dipaparkan pada dokumen kewangan :   1. Tarikh sedia, semak dan lulus 2. Nama pegawai penyedia, penyemak dan pelulus 3. Jawatan pegawai penyedia, penyemak dan pelulus |  |  |  | Salinan Pesanan Tempatan/ Baucar Bayaran/ Baucar Jurnal |
| **5.** | **Bayaran dan Terimaan Secara Elektronik**  Agensi menggunakan kemudahan perbankan elektronik. | | | | |
| **(a)** | Adakah agensi membuat pembayaransecara Pindahan Dana Elektronik(EFT)?  Jika ya, nyatakan:   1. Nisbah EFT kepada cek (Contoh: 90:10) 2. Justifikasi sekiranya nisbah EFT kepada cek kurang daripada 90%.   Nota : Pembayaran dibuat melalui portal bank juga diterima. |  |  |  | Paparan skrin urutan proses pembayaran EFT  **Atau**  SOP pembayaran melalui portal bank |
| **(b)** | Adakah notifikasi pembayaran dihantar kepada penerima? Jika ya, nyatakan kaedah yang digunakan. |  |  |  | Paparan skrin notifikasi pembayaran EFT melalui email/sms  **Atau**  Paparan skrin notifikasi pembayaran EFT di portal pembekal (Suppliers Portal)/ portal kakitangan (Staff Portal)  **Atau**  SOP penghantaran notifikasi pembayaran secara manual  Surat Lantikan Pegawai bertanggungjawab |
| **(c)** | Adakah agensi mempunyai terimaan secara elektronik?  Jika ya, nyatakan kaedah terimaan yang digunakan |  |  |  | Senarai terimaan elektronik/ perbankan internet  Paparan skrin urutan proses untuk memperakaunkan terimaan elektronik  **Atau**  SOP memperakaunkan terimaan secara elektronik |
| **6.** | **Penyesuaian Bank**  Penyata penyesuaian bank disediakan pada setiap bulan. | | | | |
| **(a)** | Adakah Penyata Penyesuaian Bank disediakan dan dijana pada setiap bulan? |  |  |  | Senarai semua bank/ akaun bank (termasuk cawangan agensi) dan kaedah penyesuaian bank (manual/ auto)  Paparan skrin modul berkaitan untuk penyediaan Penyata Penyesuaian Bank  Salinan Penyata Penyesuaian Bank terkini yang dijana daripada sistem |
| **(b)** | Adakah penyata bank boleh dimuat naik/ dikunci masuk ke dalam sistem? Nyatakan kaedah padanan. |  |  |  | Paparan skrin urutan proses muat naik/ kunci masuk penyata bank ke dalam sistem |
| **(c)** | Adakah agensi mengambil tindakan ke atas item belum selesai di Penyata Penyesuaian Bank? |  |  |  |  |
| **7.** | **Penjanaan Penyata Kewangan dan Laporan**  Penyata Kewangan dapat disediakan secara bulanan dan tahunan. | | | | |
| **(a)** | Adakah Penyata Kewangan berikut boleh disediakan pada setiap tahun:   1. Penyata Prestasi Kewangan/ Penyata Pendapatan Komprehensif? 2. Penyata Kedudukan Kewangan? 3. Penyata Aliran Tunai? 4. Penyata Perubahan Aset Bersih/ Ekuiti?   Nota : Sistem aplikasi agensi berupaya menjana Penyata Prestasi Kewangan dan Penyata Kedudukan Kewangan. |  |  |  | Salinan Penyata Kewangan yang dijana pada akhir tahun |
| **(b)** | Bagi penutupan tahunan, adakah sistem secara automatik berupaya:   1. Menyifarkan akaun bagi item Penyata Prestasi Kewangan/ Penyata Pendapatan Komprehensif? 2. Membawa baki akaun ke tahun hadapan bagi item Penyata Kedudukan Kewangan? |  |  |  | Paparan skrin “baki akhir” tahun sebelum dan “baki awal” tahun semasa Penyata Prestasi/ Pendapatan  Paparan skrin “baki akhir” tahun sebelum dan “baki awal” tahun semasa Penyata Kedudukan |
| **(c)** | Adakah Penyata Kewangan yang disediakan betul dan tepat? |  |  |  | Salinan Penyata Kewangan yang dijana melalui sistem (jumlah amaun disemak silang) |
| **(d)** | Adakah agensi menyediakan laporan lain yang diperlukan? Nyatakan laporan tersebut. |  |  |  | Salinan imbangan duga bulan terkini  Salinan laporan yang disediakan (Contoh: Laporan Pengumuran (*Ageing Report)*, Daftar Bil dan lain-lain) |
| **(e)** | Adakah agensi membuat serahan wang tak dituntut mengikut Akta Wang Tak Dituntut 1965 (Akta 370)?  Jika tidak berkenaan, sila abaikan soalan ini. |  |  |  | Surat serahan WTD daripada agensi  Surat pengesahan serahan WTD daripada JANM |
| **8.** | **Penyimpanan Data (Storan)**  Rekod kewangan disenggara dan dapat diakses pada bila-bila masa. | | | | |
| **(a)** | Adakah agensi menyimpan data/ dokumen kewangan mengikut tempoh penyimpanan yang ditetapkan oleh peraturan yang berkuat kuasa? Nyatakan tempoh penyimpanan data/ dokumen. |  |  |  | Paparan skrin kapasiti storan dan peratus penggunaan storan terkini |
| **(b)** | Adakah data/ dokumen kewangan dapat dicapai pada bila-bila masa? Nyatakan kaedah penyimpanan. |  |  |  | Sampel dokumen kewangan di sistem bagi 2 tahun dan ke atas (contoh: Baucar, Resit)  Sampel laporan jejak audit di sistem bagi 2 tahun dan ke atas |

**Disediakan Oleh**:

Bahagian Kewangan

……………………………………..

Nama :

Jawatan :

Tarikh :

**Disahkan Oleh**:

Bahagian Kewangan

………………………………………..

Nama :

Jawatan :

Tarikh :

Tandakan (√) pada ruangan **‘YA’** atau **‘TIDAK’** dan catatan/ ulasan boleh diisi di ruangan **‘CATATAN AGENSI’**.

| **BIL** | **KRITERIA PEMATUHAN SAGA** | **YA** | **TIDAK** | **CATATAN AGENSI** | **DOKUMEN SOKONGAN** |
| --- | --- | --- | --- | --- | --- |
| **B. KRITERIA TEKNIKAL** | | | | | |
| **1.** | **Pentadbiran Profil Keselamatan Pengguna**  Sistem aplikasi perakaunan dan kewangan mempunyai Pentadbiran Profil Keselamatan Pengguna | | | | |
| **(a)** | 1. Adakah agensi melantik pentadbir sistem untuk sistem aplikasi perakaunan dan kewangan di agensi? 2. Adakah agensi melantik sekurang-kurangnya satu (1) pentadbir sistem? |  |  |  | Surat Lantikan Pentadbir Sistem yang ditandatangani oleh Ketua/ Pengarah Bahagian(yang tidak terlibat dalam operasi sistem aplikasi perakaunan dan kewangan agensi) |
| **(b)** | Adakah agensi mempunyai *Standard Operating Procedure* (SOP) bagi pentadbiran pengguna? |  |  |  | SOP Pentadbiran Profil Keselamatan Pengguna |
| **(c)** | Adakah SOP pentadbiran pengguna mempunyai maklumat berikut:   1. Penerangan mengenai tatacara pendaftaran pengguna, pengemaskinian tahap capaian/ hak modul dan peranan, had kuasa kelulusan pengguna serta penamatan ID? 2. Borang permohonan pendaftaran pengguna, pengemaskinian tahap capaian/ hak, had kuasa kelulusan serta penamatan ID? 3. Carta alir tatacara pendaftaran pengguna, pengemaskinian tahap capaian/ hak, had kuasa kelulusan serta penamatan ID? 4. Tarikh kemas kini dokumen? |  |  |  |
| **(d)** | Adakah agensi mempunyai borang pentadbiran profil keselamatan pengguna yang merekodkan maklumat berikut:   1. Pendaftaran ID? 2. Tahap capaian/ hak modul dan peranan? 3. Had kuasa kelulusan? 4. Penamatan ID? 5. Tarikh kuat kuasa? |  |  |  | Salinan Borang Capaian Pengguna Sistem yang telah diluluskan |
| **(e)** | Adakah sistem aplikasi perakaunan dan kewangan mempunyai kemudahan pentadbiran profil keselamatan untuk mengkonfigurasi dan menyenggara setiap capaian pengguna di sistem? |  |  |  | Paparan skrin senarai pengguna dan capaian/ had kuasa |
| **(f)** | Adakah setiap pengguna dibekalkan dengan satu ID dan ID tersebut adalah unik seperti nama singkatan, nombor kad pengenalan atau nombor pekerja? Nyatakan. |  |  |  | Paparan skrin bukti ID adalah unik |
| **(g)** | Adakah ID pengguna yang berstatus *inactive* tidak akan dihapuskan (dalam sesuatu tempoh mengikut dasar keselamatan agensi) bagi membolehkan rekod jejak audit diekstrak apabila diperlukan?  Nota: ID pengguna boleh dihapuskan dari pangkalan data dalam proses pengemasan (housekeeping) mengikut tempoh yang bersesuaian. |  |  |  | Paparan skrin bukti ID ditukar kepada status *inactive*  Laporan jejak audit pengguna sebelum dan selepas tarikh kuat kuasa penamatan |
| **2.** | **Jejak Audit(Audit Trail)Daripada Sistem**  Sistem aplikasi perakaunan dan kewangan mempunyai jejak audit bagi merekod semua aktiviti pengguna yang merangkumi ID pengguna, modul yang diakses serta tarikh dan masa bagi setiap aktiviti termasuk log masuk dan log keluar. | | | | |
| **(a)** | Adakah sistem aplikasi perakaunan dan kewangan mempunyai fungsi jejak audit?  Nota: Setiap aktiviti yang dilakukan perlu direkod mengikut kronologi bagi tujuan mengesan jejak audit. |  |  |  | Paparan skrin Laporan Jejak Audit terkini berdasarkan modul  Paparan skrin Laporan Jejak Audit terkini berdasarkan ID (login pengguna) |
| **(b)** | Adakah sistem aplikasi perakaunan dan kewangan merekod setiap aktiviti pengguna di dalam sistem seperti berikut:   1. ID Pengguna? 2. Tarikh dan Masa Transaksi? 3. Jenis Transaksi? 4. Modul yang Diakses? 5. Maklumat log masuk dan log keluar? |  |  |  |
| **3.** | **Sistem Log**  Sistem aplikasi perakaunan dan kewangan mempunyai sistem log bagi merekodkan semua aktiviti capaian ke atas aplikasi dan pangkalan data. | | | | |
| **(a)** | Adakah sistem log dipasang/ dikonfigurasi di server/ komputer untuk merekod semua aktiviti capaian ke atas aplikasi dan pangkalan data?  Nota: Setiap aktiviti capaian perlu direkod bagi tujuan mengesan ralat atau wujudnya aktiviti lain yang tidak sah. Jejak audit dan log sistem hendaklah dilog dan integriti dilindungi dari perubahan yang disengaja atau tidak disengajakan, dipantau setiap hari untuk mengesan aktiviti luar biasa dan disimpan dalam tempoh yang disarankan oleh Arkib Negara. |  |  |  | Paparan skrin log aplikasi dan pangkalan data |
| **(b)** | Adakah sistem log mempunyai maklumat berikut:   1. Alamat IP Pengguna? 2. Tarikh dan Masa Transaksi? |  |  |  |
| **(c)** | Adakah laporan log boleh dijana dan diekstrak sendiri oleh agensi? |  |  |  | Paparan skrin urutan proses mengekstrak log server bagi Microsoft Windows:  (1)Open “Event Viewer”  (2)Klik “Log” to export (\*.evt)  (3)Klik kanan “Log” dan “Save All Event As ...” |
| **(d)** | Adakah laporan log disemak bagi mengenalpasti capaian IP yang meragukan? |  |  |  |
| **4.** | **Keselamatan Maklumat Dalam Rangkaian dan Infrastruktur ICT**  Sistem aplikasi perakaunan dan kewangan mestilah mempunyai ciri-ciri keselamatan dalam penyediaan rangkaian serta infrastruktur ICT | | | | |
| **(a)** | Adakah sistem aplikasi dipasang di server atau komputer khas yang bertindak sebagai server? Nyatakan lokasi penempatan server / komputer khas.  Sekiranya sistem aplikasi ditempatkan di bilik server atau pusat data, adakah agensi telah menerima khidmat nasihat daripada Pejabat Ketua Pegawai Keselamatan Negara (CGSO)? |  |  |  | Surat/emel permohonan khidmat nasihat kepada CGSO  Surat/emel maklumbalas khidmat nasihat daripada CGSO untuk tiga (3) aspek keselamatan iaitu:   * 1. Keselamatan dokumen/ pengkelasan;   2. Keselamatan fizikal/ persekitaran; dan   3. Keselamatan personel |
| **(b)** | Adakah *Network Diagram* mempunyai maklumat berikut:   1. Fizikal perkakasan yang terlibat dengan akses ke sistem aplikasi perakaunan dan kewangan (termasuk sistem yang berintegrasi) dan kemudahan sandaran data (backup facilities)? 2. Logikal diagram sekiranya perkakasan menggunakan pendekatan *virtual machines* (termasuk sistem yang berintegrasi) dan kemudahan sandaran data(backup facilities)? 3. *Network segmentation* berserta ciri-ciri keselamatan rangkaian? 4. Capaian rangkaian dari cawangan/ subsidiari (yang mengakses ke sistem aplikasi perakaunan dan kewangan atau sistem yang berintegrasi - jika berkaitan)? 5. Pusat Data (DC) dan Pusat Pemulihan Bencana (DRC)? |  |  |  | *Network Diagram* |
| **(c)** | **Sila jawab soalan ini jika sistem aplikasi perakaunan dan kewangan berasaskan web (web-based):**   1. Adakah sistem aplikasi perakaunan dan kewangan dilengkapkan dengan *Secure Socket Layer* (SSL) dan algorithma yang digunakan adalah sekurang-kurangnya sha-2 (secure hash algorithm)? 2. Adakah sistem sokongan berasaskan web (web-based) yang berintegrasi dengan sistem aplikasi perakaunan dan kewangan (web-based) dilengkapkan dengan SSL?   **Sila jawab soalan ini jika sistem aplikasi perakaunan dan kewangan adalah berasaskan klien (client-based):**   1. Adakah capaian pengguna ke atas sistem aplikasi perakaunan dan kewangan dari luar kampus rangkaian agensi menggunakan *Virtual Private Network* (VPN) atau pendekatan lain yang setara? 2. Adakah sistem sokongan (web-based) yang berintegrasi dengan sistem aplikasi perakaunan dan kewangan (client-based) dilengkapkan dengan SSL? |  |  |  | Paparan skrin URL sistem di *browser*  Paparan skrin *SSL Certificate*  Paparan skrin *VPN Login*  Paparan skrin *SSL Certificate*  Paparan skrin URL sistem di *browser* |
| **5.** | **Penamatan Sesi Secara Automatik (Auto Logoff)**  Sistem aplikasi perakaunan dan kewangan mempunyai keupayaan untuk menamatkan aplikasi secara automatik (auto logoff) dan/ atau membuat *computer lock* (screen saver dengan kata laluan) | | | | |
| **(a)** | Adakah sistem aplikasi perakaunan dan kewangan mempunyai fungsi untuk menamatkan sesi secara automatik (auto logoff) sekiranya pengguna tidak aktif bagi sesuatu tempoh yang ditetapkan?  Jika ya, nyatakan tempoh penamatan sesi secara automatik (auto logoff) yang ditetapkan.  Jika tidak, adakah agensi menetapkan *screen lock* secara automatik? Nyatakan tempoh yang ditetapkan. |  |  |  | Paparan skrin penetapan *auto logoff*  Paparan skrin yang membuktikan *auto logoff* berfungsi mengikut tempoh yang ditetapkan |
| **(b)** | Adakah agensi berkeupayaan untuk menukar tetapan penamatan sesi secara automatik (auto logoff)? |  |  |  | Paparan skrin penetapan *auto logoff* |
| **(c)** | Adakah tempoh penamatan sesi secara automatik (auto logoff) dinyatakan dalam polisi agensi seperti Dokumen Keselamatan ICT (DKICT)? |  |  |  | Cabutan DKICT mengenai tempoh penamatan sesi secara automatik  Salinan polisi yang lain yang berkaitan |
| **6.** | **Sandaran Data (Backup) Dan Pengujian *Restore* Secara Berkala**  Aplikasi dan data bagi sistem perakaunan dan kewangan dibuat sandaran data (backup) secara berkala. | | | | |
| **(a)** | Adakah agensi mempunyai *Standard Operating Procedure* (SOP) bagi pengendalian sandaran data (backup)dan *restore* untuk sistem aplikasi perakaunan dan kewangan? |  |  |  | SOP Sandaran Data (Backup) & *Restore*  Salinan Borang-Borang Permohonan  Carta Alir Sandaran Data (Backup) & *Restore* |
| **(b)** | Adakah *Standard Operating Procedure* (SOP) sandaran data (backup) mengandungi maklumat berikut:   * 1. Media sandaran data (backup) yang digunakan?   2. Kekerapan sandaran data (Contoh: harian, bulanan, tahunan)?   3. Kaedah sandaran data (Contoh: *incremental backup*, *full backup*, automatik, manual)?   4. Penempatan/ penyimpanan media sandaran data (backup) di lokasi luar premis?   5. Prosedur pengendalian media sandaran data (backup) meliputi penyediaan, penghantaran, penyimpanan, penggunaan dan pelupusan dilaksanakan mengikut DKICT, Arahan Keselamatan, Arahan Teknologi Maklumat dan/ atau Akta Arkib Negara? |  |  |  |
| **(c)** | Adakah terdapat kemudahan sistem sandaran data(backup)yang menyokong dan melindungi sistem aplikasi perakaunan dan kewangan agensi? Nyatakan media sandaran (backup) yang digunakan.  Contoh media sandaran (backup):   1. *Network-Attached Storage* (NAS)/ *Storage Area Network* (SAN) 2. *Server Replication* 3. *Tape* 4. Lain-lain : *External Hard Disk*/ *Pendrive*/ CD/ Micro SD dan lain-lain (nyatakan) |  |  |  | Paparan skrin log *backup* |
| **(d)** | Adakah prosedur sandaran data (backup) dibuat secara berkala? Nyatakan kekerapan pelaksanaan *backup.* (contoh: harian, mingguan atau bulanan). |  |  |  | Buku log sandaran data (backup) |
| **(e)** | Adakah salinan sandaran data (backup) disimpan di luar premis agensi dan lokasi merupakan premis Kerajaan? Nyatakan lokasi dan kekerapan penghantaran. |  |  |  | Gambar lokasi penyimpanan sandaran data (backup)  Buku log sandaran data (backup) |
| **(f)** | Adakah terdapat kawalan keselamatan ke atas pengendalian media sandaran data (backup) di luar premis? Nyatakan.  Contoh:   1. Peti besi berkunci 2. Kawalan keselamatan lokasi penyimpanan 3. Pegawai bertanggungjawab 4. Rekod log aktiviti |  |  |  | Gambar peti besi berkunci  Gambar kawalan keselamatan lokasi penyimpanan media sandaran (backup)  Buku atau laporan log aktiviti |
| **(g)** | Adakah prosedur pengujian *restore* bagi semua media sandaran data (backup) diuji sekurang-kurangnya satu (1) kali setahun? |  |  |  | Borang Permohonan Pengujian *Restore*  Laporan aktiviti *restore* |
| **(h)** | Adakah data kewangan sebelum dan selepas *restore* disemak dan disahkan oleh pegawai kewangan? |  |  |  | Imbangan Duga sebelum dan selepas *restore*  (di server produksi) yang mempunyai tarikh, masa dan telah disahkanoleh pegawai kewangan |
| **7.** | **Pelan Pemulihan Bencana (*Disaster Recovery Plan*-DRP)**  Agensi Kerajaan mempunyai Pelan Pemulihan Bencana (DRP) bagi sistem aplikasi perakaunan dan kewangan yang digunakan. | | | | |
| **(a)** | Adakah agensi mempunyai Pelan Pemulihan Bencana (DRP) untuk sistem aplikasi perakaunan dan kewangan? |  |  |  | *Disaster Recovery Plan (DRP)* |
| **(b)** | Adakah Pelan Pemulihan Bencana (DRP) mempunyai maklumat berikut:   * 1. Struktur Organisasi Pasukan DRP (*DR Team*)?   2. Prosedur/ tatacara bagi tiga fasa minimum iaitu fasa normal (perlu mempunyai penerangan berkaitan strategi simulasi), fasa pemulihan bencana dan fasa selepas bencana?   3. *Recovery Point Objective* (RPO) yang sepadan dengan strategi *backup?*   4. *Recovery Time Objective* (RTO) yang sepadan dengan jumlah masa diambil dalam fasa pemulihan dan jenis DRC?   5. Maklumat lokasi dan jenis DRC sama ada *cold, warm atau hot?*   6. Strategi menangani kehilangan data?   Nota: Pelan ini bertujuan memastikan pemulihan bencana dapat dilakukan segera dengan kehilangan data yang minimum. |  |  |  |
| **(c)** | Adakah pengisytiharan bencana dilakukan oleh Ketua/ Timbalan Agensi? |  |  |  | DR Team |
| **(d)** | Adakah DRP diuji sekurang-kurangnya satu (1) kali setahun?  Nota : Sekiranya jenis DRC adalah ”Cold” dan tidak mempunyai perkakasan utama, simulasi DRP menggunakan *testing environment* di Pusat Data adalah dibenarkan.  Nota: Ada 3 jenis kategori DRC:   |  |  |  |  | | --- | --- | --- | --- | | **JENIS** | **PENERANGAN** | **KOS** | **RISIKO KEHILANGAN DATA** | | Hot | Real time (RTO/RPO)-lost data dalam 15minit – kedua-dua server bagi production dan DRC online pada masa yang sama | Tinggi | Rendah | | Warm | Server di DRC akan *up* apabila server di production *down.* | Sederhana | Sederhana | | Cold | pegawai perlu pergi ke lokasi untuk up server  secara manual apabila berlaku bencana. | Rendah | Tinggi | |  |  |  | Laporan Pengujian DRP  Notis Pengisytiharan Bencana  Notis Penamatan Bencana  Laporan Penilaian Bencana |
| **(e )** | Adakah laporan DRP mempunyai maklumat berikut:   1. Notis Pengisytiharan Bencana? 2. Notis Penamatan Bencana? 3. Laporan Penilaian Bencana? |  |  |  |
| **(f)** | Adakah tempoh sebenar RPO dan RTO semasa simulasi bersesuaian dengan tempoh yang dinyatakan dalam dokumen DRP? |  |  |  | Laporan perbandingan masa antara tempoh sebenar dengan tempoh yang dinyatakan dalam dokumen DRP |
| **(g)** | Adakah data kewangan sebelum dan selepas simulasi DRP disemak dan disahkan oleh pegawai kewangan? |  |  |  | Imbangan Duga sebelum dan selepas *restore* (di server produksi) yang mempunyai tarikh, masa dan telah disahkanoleh pegawai kewangan  Imbangan Dugaselepas *restore* yang **telah mempunyai transaksi** dan disahkan oleh pegawai kewangan |

**Disahkan Oleh**:

Bahagian Teknologi Maklumat

………………………………………..

Nama :

Jawatan :

Tarikh :

**Disediakan Oleh**:

Bahagian Teknologi Maklumat

………………………………………..

Nama :

Jawatan :

Tarikh :