|  |  |  |
| --- | --- | --- |
| C:\Users\Admin\Pictures\JATA KPM.png  **BAHAGIAN PENDIDIKAN DAN LATIHAN TEKNIK VOKASIONAL**  **KEMENTERIAN PENDIDIKAN MALAYSIA**  **ARAS 5 & 6, BLOK E14, KOMPLEKS E,**  **PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN**  **KERTAS PENERANGAN**  ***(INFORMATION SHEET)*** | | |
| **KOD DAN NAMA NOSS** | IT-010-3:2016 PEMBANGUNAN APLIKASI | |
| **TAHAP** | 3 | |
| **KOD, NAMA CU DAN WA NOSS** | **CU03 / WA4 - COMMIT MODULE INTEGRATION CODE** | |
| **NAMA PROGRAM KV** | SISTEM PENGURUSAN PANGKALAN DATA DAN APLIKASI WEB | |
| **KOD DAN NAMA KURSUS KSKV** | KPD 2042 BACKUP STRATEGIES MANAGEMENT | |
| **NO.DAN TAJUK STANDARD KANDUNGAN KSKV** | K4 PRODUCE REPORT | |
| **NO. KOD NOSS** | IT-010-3:2016-C03/ P(19/19) | Muka Surat : 1  Drp : 11 |
| **NO. KOD KSKV** | KPD 2042 / P (7/7) |

**TAJUK/** *TITLE***:**

**PENULISAN LAPORAN DAN ISU PENYELENGGARAAN**

**TUJUAN/** *PURPOSE*:

Kertas penerangan ini adalah bertujuan menerangkan mengenai:

1. Kenal pasti format laporan
2. Tentukan isu penyelenggaraan

***4.0    REPORT WRITING***Apabila kegagalan berlaku, ia biasanya mula dikenalpasti di peringkat peralatan dengan unit operasi atau pengeluaran. Apabila kerosakan berlaku, setiap masalah yang berlaku perlu direkodkan. Ia mengambil masa untuk memulihkan peralatan dari kerosakan. Tempoh masa yang diperlukan kemudian untuk menentukan *MTBF (mean time between failure)* dan *MTTR (mean time to repair)*.  
 **Bila kerosakan berlaku?**Tarikh dan masa kerosakan berlaku perlu direkodkan.Ini penting untuk mengenalpasti tarikh dan masa sebelum kerosakan berlaku,tarikh *preventive maintenance* dan *corrective maintenance.*

**Dimana kerosakan berlaku?**Mendokumentasikan mana kegagalan yang berlaku dilakukan dengan memasukkan permintaan kerja *(request job order)* dalam sistem menggunakan objek teknikal yang betul (lokasi atau rekod peralatan). Selalunya pengguna sistem mendapati lebih mudah untuk hanya menulis permintaan kerja ke beberapa lokasi yang mudah diingati, dan bukannya mencari tempat yang betul di dalam sistem.

Ia adalah lebih baik untuk menggunakan tahap yang paling rendah sesuai dalam hierarki seperti rekod yang termasuk item dikekalkan sebenar dan bukannya lokasi tahap yang lebih tinggi atau subsistem. Juga, pengendali perlu memastikan untuk menunjukkan bahawa kegagalan ada di beberapa fesyen, dengan menggunakan sama ada tertentu Jenis pembuatan permintaan / kiriman, menetapkan petunjuk kepada kerja-kerja permintaan / perintah atau memasukkan maklumat kegagalan tambahan atas permintaan kerja / perintah.

Mempunyai maklumat ini dalam sistem membolehkan untuk membezakan penggantian komponen yang disebabkan oleh peristiwa kegagalan yang berkaitan dari orang-orang yang tidak penggantian bukan kegagalan. Kebolehpercayaan analisis boleh terjejas dengan merawat titik data sebagai acara kegagalan apabila ia sepatutnya telah dianggap sebagai sesuatu yang lain, seperti penggantian komponen tanpa kegagalan (atas sebab-sebab lain).Ia mungkin yang terbaik untuk digunakan khusus jenis permintaan kerja atau perintah jenis yang melaporkan kegagalan peralatan atau pincang tugas. Ini akan memudahkan analisis masa depan data sejarah kerja; jika tidak, ia akan menjadi lebih sukar untuk memahami kos dan buruh yang diperlukan untuk membuat pembaikan. Ini kerja permintaan / tempahan boleh diasingkan daripada aktiviti-aktiviti lain seperti penyelenggaraan pencegahan (PM), penyelenggaraan ramalan (PDM ), penyelenggaraan rutin, penambahbaikan, dan lain-lain Dalam sesetengah sistem, terdapat penunjuk yang unik untuk menunjukkan bahawa kegagalan yang wujud. **Bagaimana kerosakan diperbaiki?**Kegagalan mungkin telah berlaku kerana sesuatu yang menjejaskan pengeluaran produk perkilangan , telah diperhatikan semasa pusingan biasa, semasa ujian rutin, atau ditemui dengan cara lain , seperti pemerhatian kebetulan. Maklumat ini adalah penting untuk menentukan sama ada strategi yang sedia ada berkesan atau jika strategi baru mungkin diperlukan.

**Apa punca kerosakan?**Tahap pertama kegagalan dipanggil "mod kegagalan" dalam ISO 14224. Ia adalah gejala yang boleh dilihat di peringkat aset peralatan. Apabila pemerhatian ini berlaku, permintaan kerja atau arahan kerja biasanya dimasukkan dalam EAM / CMMS . Sama seperti ibu bapa membawa anak mereka ke klinik, semua yang diketahui pada masa ini adalah gejala .Tiada laporan atau analisis terperinci berlaku pada ketika ini. Sebagai contoh, pengendali boleh melaporkan bahawa pam gagal untuk memulakan . Ini dilakukan dengan menerangkan masalah ini dan memilih kod yang betul untuk memasuki mod kegagalan dalam sistem. Oleh kerana tanda-tanda yang agak generik, senarai yang sama kod boleh biasanya digunakan untuk semua jenis peralatan. **Apa kesan kepada kerosakan?**Biasanya, orang yang melaporkan kegagalan itu mempunyai beberapa idea tentang kesan kegagalan pada organisasi. Mungkin terdapat tiada kesan, atau kegagalan itu boleh menjejaskan alam sekitar, keselamatan atau pengeluaran. Maklumat ini bukan sahaja berguna di mengutamakan apa-apa tindakan susulan yang berikutnya tetapi juga bantuan penting mematuhi melaporkan kepada pihak ketiga seperti agensi kawal selia alam sekitar atau keselamatan. Jika boleh, nyatakan tahap kegagalan atau kehilangan fungsi. Peralatan yang mengalami kerosakan, tetapi setakat apa yang dilakukan oleh kerosakan peralatan? Adakah ia satu kegagalan "lengkap", seperti apabila pam gagal untuk bermula? Adakah ia satu "sebahagian" kegagalan, seperti apabila pam tidak boleh mengekalkan kadar aliran yang dikehendaki? Adakah ia satu "potensi" atau "tersembunyi" kegagalan? Walaupun ini mungkin tidak kelihatan seperti kegagalan yang sebenar kerana ia mengakibatkan daripada keadaan kejadian yang tidak mencetuskan kesalahan yang aktif, ia mungkin bahawa mereka akan berbuat demikian pada satu titik masa depan. Mengkategorikan acara-acara ini dengan betul menyokong membangunkan strategi pengurangan lebih baik di masa hadapan.

**Garis panduan penulisan laporan kerosakan.**a) Tuliskan kerja permintaan / untuk aset peralatan  
  
b) Menunjukkan bahawa kegagalan wujud  
  
c) Pilih kod yang betul untuk memasuki mod kegagalan  
  
d) Nota yang mendapati kegagalan dan bagaimana kegagalan telah ditemui.  
  
e) Huraikan masalah  
  
f) Secara pilihan , menunjukkan kesan operasi dan darjah kegagalan

**4.1 MENGHASILKAN LAPORAN SANDARAN**

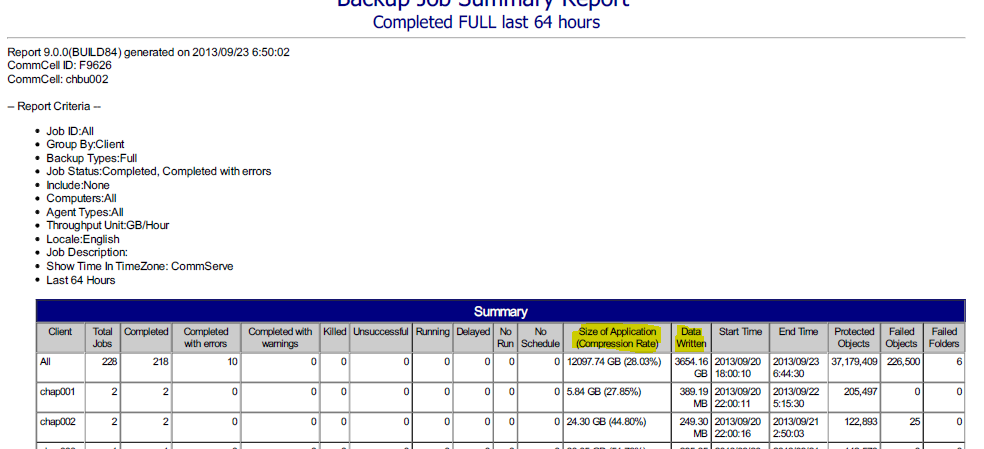
Laporan status sandaran menyediakan maklumat tentang masa lalu setiap kerja sandaran *(backup)* yang telah dilaksanakan dalam tempoh masa yang ditentukan, dan menunjukkan berapa jumlah data yang disandarkan.

Laporan status sandaran (*backup*) tidak mempunyai format yang khusus, bergantung kepada *Standard Operation Procedure (SOP*) yang telah ditetapkan oleh sesebuah syarikat.

Jadual 1 menyenaraikan dan menerangkan data yang tersedia dalam Laporan status sandaran (*backup*), dan menunjukkan sama ada setiap lajur diperlukan atau pilihan.

| **Backup Status Report Data Column** | **Description** | **Required** | **Optional** |
| --- | --- | --- | --- |
| Vault | Name of the vault where the backup data is saved |  | ✓ |
| Site | Site of the backup |  | ✓ |
| Computer | Computer or environment that was backed up | ✓ |  |
| Job | Name of the backup job | ✓ |  |
| OS Version | Operating system of the computer or environment that was backed up |  | ✓ |
| Agent Type | Type of Agent that ran the backup |  | ✓ |
| Backup Date | Date and time when the backup started |  | ✓ |
| Deleted At | If the backup data has been deleted, date and time when the safeset was deleted from the vault |  | ✓ |
| Backup Duration | Length of time that the backup ran |  | ✓ |
| Last Backup Original Size (GB) | Amount of data that was backed up from the computer or environment, in gigabytes |  | ✓ |
| Delta Size (MB) | Amount of changed data extracted during the backup, before compression, in megabytes |  | ✓ |
| Result | Outcome of the backup session: Successful or Failed | ✓ |  |

Jadual 1 : Senarai Laporan status sandaran (*backup*),

Rajah 1 menunjukkan contoh laporan bagi proses sandaran yang telah dijalankan:

Rajah 1 : Contoh laporan bagi proses sandaran (*backup*)

**4.2 ISU-ISU PENYELENGGARAAN**

1. Sandaran (***Backup*) anda tidak berfungsi.**

Sebelum membuat sebarang perubahan pada sistem pengeluaran (*production system*) anda, pastikan (*backup*) anda berfungsi. Menjalankan beberapa pemulihan ujian jika ingin memadam data kritikal. Sebelum proses sandaran (*backup*), anda mungkin ingin memastikan anda telah memilih [lokasi sandaran yang betul](http://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/selecting-a-backup-location/" \t "_blank" \o "Memilih Lokasi Cadangan).

2. **Penggunaan cakera tidak mencukupi atau tidak sesuai.**

Jangan gunakan sistem pengeluaran anda sebagai sistem arkib. Padam log lama, e-mel, dan versi perisian tidak digunakan lagi supaya isu keselamatan yang disebabkan oleh pengisian versi lama dapat dielakkan. Jejak data yang lebih kecil membolehkan pemulihan yang lebih pantas. Jika penggunaan anda melebihi 90% daripada kapasiti cakera, sama ada mengurangkan penggunaan atau menambah lebih banyak storan. Jika *partition* anda mencapai 100%, pelayan anda mungkin berhenti bertindak balas, jadual pangkalan data boleh rosak dan data mungkin hilang.

3. **Kurang pemantauan terhadap**RAID**.**

Semua pelayan pengeluaran (*production server*) harus menggunakan RAID. Adalah penting untuk mengawasi status RAID. Kegagalan pelayan yang lengkap dapat menjadikan proses penggantian drive mudah ke dalam senario pemulihan yang lama.

4. Tidak mengemaskini **OS dengan kerap.**

Kemas kini untuk sistem Linux sering dikeluarkan. Jika menggunakan sistem pengoperasian (OS) boleh mendatangkan risiko. Itulah sebabnya perlu menggunakan alat pengurusan *patch* automatik dan memantau status sistem untuk memaklumkan apabila sistem pengoperasian sudah lama tidak dikemaskini. Sekiranya anda mengemas kini pelayan anda secara manual (atau jarang), anda mungkin terlepas kemas kini keselamatan (*security updates*) yang penting. *Hackers* sering mengimbas sistem yang mempunyai kelemahan atau tidak kemaskini dalam masa beberapa jam setelah isu didedahkan.

5. Tidak mengemaskini **Panel Kawalan (*control panel*) dengan kerap.**

Jika anda menggunakan panel kawalan atau pelayan kawalan, pastikan anda mengemas kini juga. Ini bukan sahaja mengemaskini panel kawalan itu sendiri, tetapi juga mengemaskini perisian yang dikendalikannya.

6.  **Tidak mengemasikini aplikasi dengan kerap.**

Merujuk kepada penyelidikan, aplikasi web menyumbang lebih daripada 95% dari semua pelanggaran keselamatan. Pastikan anda mengemaskini aplikasi web anda, terutamanya *platform* popular seperti WordPress.

7.A**lat pengurusan jauh tidak berfungsi.**

Sekiranya pelayan diletakkan bersama atau dengan pembekal pelayan, anda perlu memastikan alat pengurusan jauh anda berfungsi. Kawalan jauh, *reboot* jauh dan mod menyelamat merupakan tiga [alat yang penting untuk pengurusan pelayan (](https://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/3-essential-server-management-tools-for-your-dedicated-server/)*[server](https://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/3-essential-server-management-tools-for-your-dedicated-server/)*[) jauh](https://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/3-essential-server-management-tools-for-your-dedicated-server/).

8.  **Perkakasan mempunyai ralat.**

Menyemak log untuk sebarang tanda masalah perkakasan. *Notification* yang terlalu panas, kesilapan membaca cakera dan kegagalan rangkaian boleh menjadi penunjuk awal terhadap kegagalan perkakasan. Ralat ini jarang berlaku tetapi perlu dititiberatkan, terutamanya jika sistem tidak berfungsi dalam keadaan normal.

9. **Penggunaan pelayan yang yang terhad .**

Sentiasa semak cakera pelayan, CPU , RAM dan penggunaan rangkaian. Jika anda mencapai had atau melebihi kapasiti, anda hendaklah merancang untuk menambah sumber ke pelayan (*server*) atau berpindah kepada pelayan yang baru.

10. **Akaun pengguna tidak dikemaskini.**

Sekira berlakunya pertukaran kakitangan, pembatalan pelanggan atau perubahan pengguna lain, mengeluarkan maklumat dan rekod daripada sistem adalah perlu agar tidak berlaku pertindihan data. Menyimpan akaun pengguna lama melibatkan keselamatan dan risiko undang-undang. Bergantung pada kontrak perkhidmatan, sesebuah organisasi atau syarikat mungkin tidak mempunyai hak untuk mengekalkan data pelanggan setelah mereka menamatkan perkhidmatan.

11. **Kata laluan tidak dikemaskini.**

Kata laluan hendaklah ditukar atau dikemaskini setiap 6 hingga 12 bulan, terutamanya jika anda telah memberikan kata laluan kepada orang lain untuk penyelenggaraan.

12. **Pemeriksa keselamatan sistem tidak berfungsi.**

Pemeriksaan berkala keselamatan pelayan (*server*) anda menggunakan alat pengauditan jauh seperti Nessus. Pemeriksaan keselamatan tetap berfungsi sebagai pemeriksaan konfigurasi sistem, kemas kini OS dan risiko keselamatan yang berpotensi. Pemeriksaan ini hendaklah dilakukan sekurang-kurangnya 4 kali setahun dan lebih baik pada setiap bulan. Selain itu, mengkaji semula [10 undang-undang pentadbiran keselamatan yang tidak berubah](http://www_ms_5b44717b2a1a6b1501da5371_pipe.bablic.com/blog/10-immutable-laws-of-security-administration-revisited/" \t "_blank" \o "10 Undang-undang Pentadbiran Keselamatan Tidak Terubah Semula).

**SOALAN** / *QUESTION* :

1. Terangkan lapan jenis isu-isu penyelenggaraan.
2. Berikan definisi laporan sandaran secara ringkas.

**RUJUKAN**/ REFERENCES :

1. Ishak, K. I. (1970, January 1). COMPUTER NETWORK SERVICES. Retrieved from http://khairulizhar.blogspot.com/.