|  |  |  |
| --- | --- | --- |
| C:\Users\User\Downloads\Telegram Desktop\photo_2018-01-15_16-09-10.jpgphoto_2018-01-15_16-09-10  **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 APPLICATION DEVELOPMENT | |
| **TAHAP** | 3 | |
| **KOD, NAMA CU DAN WA NOSS** | **CU03 / WA3 - TEST MODULE INTEGRATION CODE** | |
| **NAMA PROGRAM KV** | SISTEM PENGURUSAN PANGKALAN DATA DAN APLIKASI WEB | |
| **KOD DAN NAMA KURSUS KSKV** | KPD2042 BACKUP STRATEGIES MANAGEMENT | |
| **NO.DAN TAJUK STANDARD KANDUNGAN KSKV** | K3 VERIFY BACKUP | |
| **NO. KOD NOSS** | IT-010-3:2016-C03/P(11/19) | Muka Surat : 1  Drp : 20 |
| **NO. KOD KSKV** | KPD2042/ P(6/7) |

**TAJUK/** TITLE:

**KETAHUI TENTANG INTEGRITI, KESULITAN DAN KESEDIAAN, PENGUJIAN UNIT SERTA AKTIVITI PENYELENGGARAAN**

**TUJUAN**/ PURPOSE:

Kertas penerangan ini adalah bertujuan menerangkan mengenai:

1. Terangkan integriti, kesulitan dan kesediaan
2. Terangkan definisi pengujian unit
3. Terangkan proses aktiviti penyelenggaraan

**3.1 PENGESAHAN PENYELENGARAAN PANGKALAN DATA DAN ISU- ISU KESELAMATAN**

Apabila selesai satu modul, pembangun sistem hanya perlu *backup* modul yang terlibat sahaja. 3 prinsip asas keselamatan ialah :

***INTEGRITY***

1. Integriti bermaksud bahawa data tidak diubah dari asal oleh orang yang tidak dibenarkan, supaya ketekalan, ketepatan, dan kesahihan data masih dikekalkan. Dalam bahasa lain, integriti cuba memastikan data yang disimpan adalah betul, tidak ada pengguna yang tidak sah atau perisian berniat jahat yang mengubahnya. Integriti berusaha untuk memastikan data dilindungi dengan selamat daripada ancaman yang disengajakan (serangan penggodam) serta ancaman yang tidak disengajakan (contohnya kemalangan).
2. Integriti boleh dicapai dengan:

* Gunakan penyulitan yang kuat (*strong encryption*) untuk penyimpanan data dan media penghantaran.
* Menerapkan pengesahan dan pengesahan yang kuat (*strong authentication*) pada setiap akses / log masuk / tindakan akaun yang digunakan. Pengesahan dan pengesahan dilakukan untuk memastikan kesahihan akses.
* Menerapkan kawalan akses *(access control)* yang ketat ke sistem, iaitu setiap akaun sedia ada harus dibatasi dalam hak aksesnya. Contohnya tidak semua mempunyai hak akses untuk diedit, yang lain hanya boleh melihatnya.

1. Contoh yang mudah dan biasa mengenai kerosakan integriti yang berkaitan dengan keselamatan maklumat ialah proses menghantar e-mel. Alice menghantar e-mel kepada Bob. Tetapi apabila e-mel dihantar, separuh melalui Eve dipintas e-mel dan mengubah kandungan e-mel dan kemudian dikemukakan kepada Bob. Bob akan berfikir bahawa e-mel adalah benar dari Alice walaupun kandungannya telah diubah oleh Hawa. Ini menunjukkan aspek integriti e-mel yang dihantar oleh Alice telah hilang / rosak.

***CONFIDENTIALITY***

1. Maksud secara ringkas sama seperti makna perkataan iaitu kerahsiaan. Kerahsiaan dalam kes ini adalah maklumat yang ada dalam sistem / pangkalan data, ia adalah rahsia dan pengguna yang tidak dibenarkan atau orang tidak dapat melihat / mengaksesnya. Atau dengan kata lain, hanya pihak yang dibenarkan dan dibenarkan boleh mengakses maklumat tersebut.
2. Kerahsiaan adalah aspek yang menjamin kerahsiaan data atau maklumat. Sistem yang digunakan untuk melaksanakan e-procurement mestilah menjamin kerahsiaan data yang dihantar, diterima dan disimpan. Kebocoran maklumat boleh mengakibatkan pembatalan proses perolehan.
3. Kerahsiaan ini boleh dilaksanakan dalam pelbagai cara, seperti menggunakan teknologi kriptografi dengan menjalankan proses enkripsi (pengekodan, pengekodan) dalam penghantaran data, pemprosesan data (*application and database*), dan penyimpanan data (*storage*). Teknologi kriptografi boleh membuat sukar untuk membaca data untuk pihak yang tidak dibenarkan.
4. Selalunya pereka dan pelaksana sistem maklumat atau sistem transaksi elektronik cuai dalam melaksanakan keselamatan. Umumnya perlindungan ini hanya dianggap pada peringkat akhir supaya keselamatan lebih sukar disepadukan dengan sistem yang ada. Penambahan dalam peringkat akhir ini menyebabkan sistem menjadi tampal. Satu lagi akibat daripada ini ialah kos lebih mahal daripada jika perlindungan telah difikirkan dan dilaksanakan dari awal.
5. Akses kepada maklumat juga perlu dilakukan melalui mekanisme kebenaran yang ketat. Tahap keselamatan mekanisme pengesahan bergantung pada tingkat kerahasiaan data yang dikehendaki.
6. Privasi: lebih kepada data yang bersifat peribadi, maklumat yang betul diakses oleh mereka yang berhak (dan bukan orang lain). Contoh: alamat e-mel pengguna tidak dapat dibaca oleh pentadbir.
7. Kerahsiaan adalah pencegahan bagi mereka yang tidak berminat untuk mencapai maklumat, berkaitan dengan data yang diberikan kepada pihak lain untuk tujuan tertentu dan hanya dibenarkan untuk tujuan tertentu.
8. Kebanyakan organisasi umumnya mengelaskan maklumat / data untuk menampung pencapaian kerahsiaan. Klasifikasi adalah penggunaan dalaman sahaja (hanya digunakan dalam persekitaran dalaman syarikat), orang awam (biasanya diedarkan melalui laman web atau media sosial syarikat), dan sulit (sangat sulit, misalnya data yang berkaitan dengan perancangan, kewangan, proses perniagaan, dll.).
9. Ancaman yang timbul daripada pihak yang tidak berminat dalam aspek kerahsiaan termasuk:

* *Password strength* (kata laluan lemah yang digunakan, begitu mudah untuk meneka atau memfitnah)
* *malware* (kemasukan virus yang boleh mencipta backdoor ke sistem atau mengumpul maklumat pengguna)
* *social engineering* (kesedaran keselamatan lemah pengguna yang sangat mudah untuk 'dibohongkan' oleh penyerang, yang biasanya adalah seseorang yang sudah tahu).

1. Kaedah umum yang digunakan untuk menjamin pencapaian aspek kerahsiaan adalah untuk melaksanakan penyulitan. Penyulitan adalah teknik untuk menukar fail / data / maklumat dari bentuk yang dapat difahami (plaintext) kepada bentuk yang tidak dapat difahami (ciphertext), sehingga sukar bagi penyerang mendapatkan maklumat yang mereka perlukan. Penyulitan mesti dilakukan pada tahap penyimpanan data dan media penghantaran.
2. Adakah anda masih ingat berita pada awal Disember 2016 mengenai penggodaman google, yahoo, dailymotion yang berjaya, yang mengakibatkan pencurian data pengguna mereka? Ini adalah contoh kerosakan kepada aspek kerahsiaan keselamatan maklumat.

***AVAILABILITY***

1. *Availability* adalah usaha untuk mencegah pengekalan maklumat atau sumber yang berkaitan oleh mereka yang tidak berhak, yang berkaitan dengan ketersediaan maklumat apabila diperlukan. Selain itu, maksud availability (ketersediaan) adalah untuk memastikan sumber-sumber yang tersedia, sedia untuk diakses pada bila-bila masa oleh pengguna / aplikasi / sistem yang memerlukannya. Sama seperti aspek integriti, kerosakan terhadap aspek ketersediaan sistem juga boleh disebabkan oleh faktor yang disengajakan dan faktor secara kebetulan.
2. Faktor yang disengajakan dapat dari *serangan Denial of Service (DoS), malware, atau hacker / cracker.* Bagi faktor kebetulan (kemalangan) boleh disebabkan kegagalan perkakasan (rosak atau tidak berfungsi dengan baik perkakasan), litar pintas, api, banjir, gempa bumi, dan bencana alam yang lain.
3. Untuk memastikan aspek ketersediaan dicapai, organisasi syarikat boleh melaksanakan:
4. (disaster recovery plan) pelan pemulihan bencana (mempunyai cadangan tempat dan sumber yang baik, jika berlaku bencana dalam sistem)
5. *(Redundant Hardware)* perkakasan berlebihan (contohnya, mempunyai banyak bekalan kuasa)
6. RAID (salah satu cara untuk menangani kegagalan cakera)
7. *(Data backup)* sandaran data (sandaran data rutin)
8. Satu contoh aspek kegagalan sistem baru-baru ini adalah wap, platform pengedaran permainan digital terbesar di dunia, yang tidak boleh diakses atau mengalami downtime server yang berpengalaman oleh serangan Penyebaran Dedarkan Perkhidmatan (DDoS).

Oleh itu, 3 prinsip asas mengenai keselamatan maklumat. Ketiga (kerahsiaan, integriti, ketersediaan) mesti dicapai dan dilindungi untuk mewujudkan sistem yang boleh dianggap selamat walaupun pada hakikatnya tidak ada sistem yang benar-benar selamat.

**PENGUJIAN**

1. Apabila sesuatu aplikasi dihasilkan, aplikasi tersebut perlu diuji. Matlamat utama pengujian adalah untuk mengesan ralat (*error*) terhadap aplikasi yang telah dibangunkan. Pendekatan pertama yang diambil dalam pengujian ialah pengujian luaran atau *black-box testing*. Pengujian luaran juga dikenali sebagai behavioral testing atau functional testing.
2. Fungsinya adalah untuk menguji tampilan antaramuka, fungsi-fungsi dalam aplikasi dan aliran fungsi dan proses bagi memastikan proses tersebut menepati dengan kehendak pengguna. Aplikasi prototaip yang telah dibangunkan perlu menjalani pengujian ini. Kemudian, pengujian dalaman atau *white-box testing* pula perlu dilaksanakan. Pengujian dalaman diperlukan untuk menguji prosedur dan laluan logikal terhadap aplikasi supaya aplikasi bebas dari ralat.
3. Pengujian terhadap antaramuka yang telah disiapkan adalah untuk meningkatkan lagi persembahan rekabentuk antaramuka. Persepsi terhadap antaramuka sangat subjektif kerana tiada formula yang tertentu yang dapat mengukur antaramuka yang terbaik. Walaubagaimanapun, pengujian sangat diperlukan bagi memastikan sistem yang dibangunkan berfungsi dengan baik. Antara elemen yang diuji ialah :
   1. Butang navigasi dan arahan
   2. Input pengguna dan Output kepada pengguna
   3. Sejauh mana pengguna mudah mempelajari dan mudah faham semasa menggunakan sistem tanpa atau dengan bantuan sokongan yang disediakan
4. Antara jenis-jenis pengujian ialah pengujian unit dan pengujian kebolehgunaan.

**3.2 *UNIT TESTING* (PENGUJIAN UNIT)**

Dalam pengaturcaraan komputer, ujian unit adalah kaedah pengujian perisian. Dalam kaedah ini unit individu kod sumber, koleksi satu atau lebih modul program komputer bersama-sama dengan kawalan data yang berkaitan, prosedur penggunaan, dan prosedur operasi, diuji untuk menentukan sama ada ia sesuai digunakan.

Kita dapat melihat unit sebagai bahagian terkecil yang dapat diuji dari aplikasi. Dalam pengaturcaraan prosedur, unit boleh menjadi satu daripada satu modul, tetapi biasanya unit adalah fungsi atau prosedur individu.

**Ujian unit** adalah tahap pengujian perisian di mana unit / komponen individu dari suatu perisian diuji. Tujuannya adalah untuk mengesahkan bahawa setiap unit perisian berfungsi seperti yang direka. Satu unit adalah bahagian yang paling kecil yang dapat diuji dari mana-mana perisian. Ia biasanya mempunyai satu atau beberapa input dan biasanya satu output.

Pegujian dilakukan terhadap unit perisian/ laman web terkecil yang dinamakan modul. Modul terdiri daripada satu fungsi atau prosedur atau satu-satu laman web. Setiap modul perlu diuji dari beberapa aspek seperti pengendali ralat, antaramuka, navigasi dan lain-lain.

Rajah 1 : Aspek pengujian

**Penerangan mengenai rajah 1.**

|  |  |
| --- | --- |
| **Aspek pengujian** | **Tugas/peranan** |
| Pengendali ralat | Menangani ralat daripada berlaku semasa pelaksanaan. |
| Laluan logik/ Navigasi | Memastikan setiap pernyataan diuji sekurang-kurangnya sekali. Memastikan navigasi/linking berjalan lancar. |
| Nilai sempadan & kelas data | Memastikan modul berfungsi dengan baik pada nilai sempadan. Kelas data yang sah dan tidak sah juga diuji. |
| Struktur data | Data yang disimpan dalam pangkalan data dapat mengekalkan integrasi, kesahihan semasa diguna pakai. |
| Antaramuka | Menyemak parameter/data/input yang masuk dan keluar daripada modul aturcara/laman web berjalan lancar |

Jadual 1 : Aspek pengujian serta tugas dan peranannya

**Faedah Pengujian Unit :**

1. Masalah boleh didapati pada peringkat awal. Oleh kerana ujian unit dijalankan oleh pemaju, mereka boleh menguji sebahagian daripada kod. oleh itu masalah boleh didapati dengan sangat awal dan boleh diselesaikan dengan segera.
2. Ujian unit membantu dalam mengekalkan / menukar kod jika ada perubahan dari aplikasi. ini mungkin dilakukan dengan membuat kod kurang, jadi unit ujian boleh dilaksanakan. Memudahkan pemaju / pengaturcara pada masa hadapan.
3. Bugs yang didapati semasa ujian unit juga membantu dengan kos penetapan bug. Bayangkan jika kos bug yang dijumpai pada peringkat akhir pembangunan sangat banyak, jadi sangat mahal untuk mengubahnya jika kita tidak tahu dari permulaan bug.
4. Ujian Unit membantu dalam memudahkan proses debugging. Jika ujian gagal maka perubahan terakhir dibuat dalam kod.
5. Dan yang terakhir adalah masa yang diperlukan dalam kerja / penyelenggaraan aplikasi lebih cepat dan lebih cekap

**3.3 PROSES AKTIVITI PENYELENGARAAN**

**MENGENALPASTI KEPERLUAN PENYELENGGARAAN KOMPUTER**

Penyelenggaraan sistem komputer yang diperlukan untuk melakukan dengan kerap untuk memastikan sistem atau perkakasan berfungsi dengan baik

Jenis penyelenggaraan komputer

Terdapat dua jenis: -

* PENCEGAHAN (*PREVENTIVE*)
* PEMBETULAN (*CORRECTIVE*)

**PREVENTIVE MAINTENANCE (PENYELENGARAAN PENCEGAHAN)**

1. Penyelenggaraan yang perlu anda lakukan untuk mengelakkan sebarang kerosakan atau kerosakan pada sistem komputer anda
2. Contoh: -
   1. Mengimbas untuk virus menggunakan mana-mana perisian anti-virus
   2. Gunakan defragmentation untuk menguruskan mana-mana fail sampah dalam Hardisk yang
   3. Pembersihan perkakasan komputer dari tanah untuk mengelakkan litar pintas
   4. Menukar kompaun haba pada pemproses untuk memastikan distrubute haba betul ke heatsink
3. Perancangan yang sistematik, dibuat secara berkala (tahunan dan sebagainya), dan tepat pada masa diperlukan seperti mencuci, melincirkan, membaiki dan menggantikan bagi komponen-komponen untuk :
4. Meminimumkan kerugian pengeluaran disebabkan oleh kerosakan-kerosakan
5. Memanjangkan harta hayat modal
6. Mengurangkan kos keseluruhan
7. Kaedah penyengaraan berdasarkan kombinasi pangkalan masa dan keadaan untuk memastikan peralatan berfungsi oleh pengawalan komponen-komponen peralatan, assemblies, subassemblies, accerssories, attachment, dan sebagainya.
8. Memelihara prestasi bahan-bahan struktur
9. Mencegah kakisan, keletihan (fatigue) dan lain-lain bentuk kemorosotan yang melemahkan mereka.
10. Untuk mencegah atau melambatkan kerosakan-kerosakan
11. Tindakan pencegahan boleh dijalankan mengikut suatu jadual pratentu dan tetap atau apabila diperlukan
12. Rancangan –rancangan penyelengaraan pencegahan yang direka dengan elok boleh mengurangkan insiden penyelengaraan kecemasan
13. Program penyelengaraan pencengahan yang dilakukan secara meluas adalah penting untuk mengurangkan kekerapan dan gangguan aliran kerja.

**Tools penyelenggaraan**

1. Cutter

2. Plier

3. Alat Crimping

4. Pemutar Skru

5. Pembersih Vakum / Blower

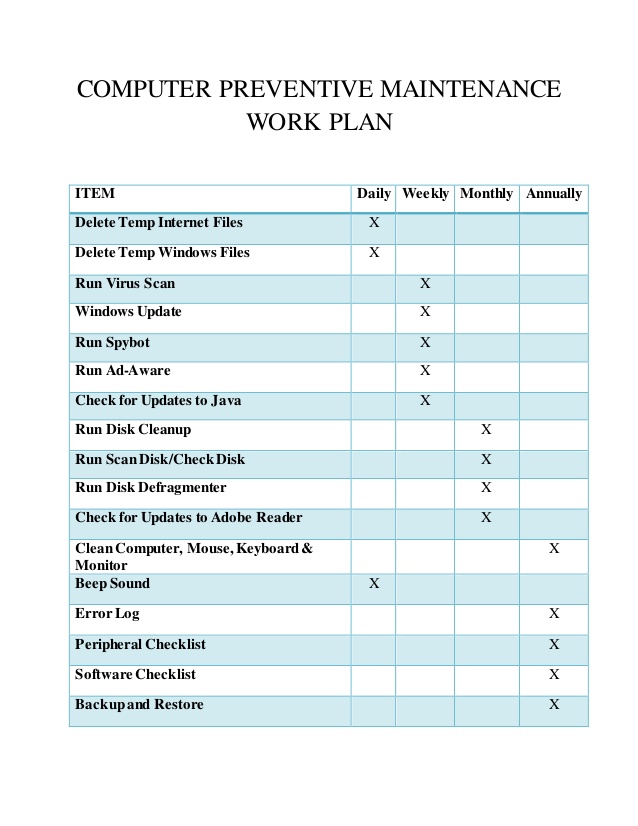
6. Kompaun Thermal

**Menjalankan komputer penyelenggaraan pencegahan**

Tugas penyelenggaraan pencegahan komputer

* Tempat Kerja dan kawasan stesen kerja pemeriksaan:
* Pengurusan - kabel
* Cleanliness
* Temperature dan kelembapan
* Hubungan -connectivity
* Power kestabilan
* Firmware komputer dan penyelenggaraan perkakasan :
* Bios
* Fan
* Memandu -optical
* Input dan output
* Bateri untuk desktop dan komputer riba
* Cakera keras –external
* Pemasangan patch perisian dan up-dating :
* Update Sistem pengendalian patch
* Update Permohonan
* Kemas kini pemandu Peranti
* Update BIOS
* BIOS a.k.a Sistem Input Output Asas. Juga dikenali sebagai "Setup Sistem", BIOS adalah satu perisian yang tinggal di dalam papan induk, biasanya dirujuk sebagai CMOS (Complementary Metal Oxide Semiconductor).
* Storan komputer penyelenggaraan Peranti :
* Status penggunaan ruang cakera
* Cakera pemeriksaan
* Defragmentation Disk
* Cakera membersihkan
* Ralat pemeriksaan
* Pemeriksaan keselamatan komputer dan mengemaskini :
* Antivirus corak sehingga tarikh
* Imbasan Ancaman dan menghapuskan
* Konfigurasi Firewall pemeriksaan
* Konfigurasi Internet pemeriksaan
* Sandaran data komputer
* Data Backup adalah proses memulihkan maklumat penting untuk mengelakkan ia daripada hilang.
* Sandaran ini adalah untuk menyelamatkan data asal dan keupayaan untuk memulihkan semua data yang hilang dengan betul dan cepat.
* Bagaimana untuk membuat sandaran data boleh dilakukan dengan pelbagai peranti, sama ada melalui cakera dalaman keras sendiri, cakera keras luaran, CD R / RW, DVD R / RW, cakera flash, memori, dan perisian sandaran yang boleh diperolehi percuma dengan memuat turun di internet dan dibayar.
* data User sandaran (dokumen)
* data –email
* Penilaian pengoptimuman prestasi komputer
* Advance penjagaan sistem :
* sejenis perisian yang mengimbas dan memastikan perisian lain atau pemandu adalah up-to-date supaya sistem anda dapat berfungsi sepenuhnya.

**Contoh Preventive Maintenance Worksheet**



Jadual 2 : Contoh Preventive Maintenance Worksheet

**CORRECTIVE MAINTENANCE (PENYELENGARAAN PEMBETULAN)**

1. Penyelenggaraan yang anda lakukan selepas sistem komputer yang disyaki kerosakan
2. Contoh: -
   1. Checking / mengubah USBport jika tetikus / papan kekunci tidak dikesan
   2. Dengan menggunakan getah atau isopropyl alkohol untuk membersihkan ram jika ram tidak mengesan / fungsi
   3. ambil perhatian: Kaedah getah seolah-olah boleh merosakkan ram jika tidak melakukannya dengan berhati-hati
   4. Sistem memulihkan jika OS (windows) mendapat ralat selepas pemasangan tertentu
3. Ia menambahbaik peralatan dan komponen-komponennya agar penyelengaraan pencegahan boleh dilaksanakan dengan pasti
4. Peralatan dengan rekabentuk daif mesti direkabentuk semula
5. Sesuai untuk barang-barang penyelengaraan yang berkos tinggi *poor maintenance* , *poor design* atau opreasi di luar spesifikasi reka bentuk
6. Pilihan yang perlu dibuat adalah di antara kos rekabentuk semula dan kos penyelengaran berulang
7. Sesetengah keadaan jika menggantikan sebuah mesin adalah lebih ekonomi daripada dibaiki maka pembaikan tidak harus dilakukan
8. Amat sesuai apabila kegagalan yang bila kronik dan berulang-ulang berlaku dan memerlukan pengubahsuaian- pengubahsuaian
9. Ia memerlukan tindakan kejuruteraan daripada tindakan penyengaraan tetapi sering menjadi tanggungjawab jabatan penyengaraan.

**Tools untuk penyelenggaraan**

1. Cutter

2. Plier

3. alat Crimping

4. pemutar skru

5. Pembersih vakum / blower

6. kompaun Thermal

**Melaksanakan penyelenggaraan komputer pembetulan**

i. Analisis laporan penyelenggaraan Sebelum

* + Aktiviti penyelenggaraan Sebelum
  + Sejarah Fault
  + Sejarah Pembetulan
  + Sejarah pengguna

ii. Jenis-jenis penggera amaran, seperti:

* + Startup beep (bip bunyi pada itu boot pc a)
  + Biasanya satu bip yang bermaksud komputer anda berada dalam keadaan yang baik
  + Lagi bip bermakna terdapat kesilapan, dan setiap ralat bergantung kepada jenis BIOS
  + Http://www.bioscentral.com/beepcodes/awardbeep.htm untuk AWARD BIOS
  + Http://www.bioscentral.com/beepcodes/phoenixbeep.htm untuk PHOENIX BIOS

iii. Jenis-jenis Power On Self Test (POST) mesej, seperti:

* + Keyboard tidak disambung
    - Tanggalkan kabel USB dan pasang semula, jika ia telah berjaya, keyboard boleh tukar yang baru.
  + Tarikh BIOS
    - Main set - sehingga utiliti untuk menetapkan tarikh dan masa.
  + Modul memori konfigurasi yang tidak betul
    - Pengguna perlu merujuk kepada panduan pengguna untuk memastikan keperluan memori
  + Processor ralat kelajuan bas
    - Kita perlu mengkonfigurasi semula pemproses yang betul

    iv. mendapatkan semula data sandaran

* + Prosedur pengambilan Data
  + Sandaran Data

v. Jenis tindakan pembetulan

* + Tindakan interruptive
  + Tindakan Bukan interruptive

vi. Jenis-jenis memulihkan

* Perisian memulihkan
* Pemulihan Permohonan
* Data memulihkan
* Konfigurasi memulihkan

  vii. Sistem komputer pemulihan:

* + Jenis-jenis perisian
    - Sistem Software
    - Bahasa Software
    - Aplikasi perisian
    - Utiliti Software
  + Jenis-jenis data
    - Antara muka Data
    - Data Ordinal
    - Data Radio
  + Kaedah Pemulihan

viii. Kos

* + Komputer kos sebahagian
  + Perkhidmatan kos / buruh

ix. Prosedur komputer sebahagian pelupusan

* + Memastikan data dimusnahkan
  + Recycling
  + Jual
  + Buang di kawasan buangan sampah digital

**SOALAN/***QUESTION*:

1. Jelaskan maksud *Preventive Maintenance* (Penyelengaraan Pencegahan) dengan betul.
2. Jelaskan maksud *Corrective Maintenance* (Penyelengaraan Pembetulan) dengan betul.
3. Terangkan **lima** aspek pengujian berserta tugas dan peranannya.

**RUJUKAN :**

1. Azaim, H., Haikal, Azaim, H., Wahyuningsih, A., Azaim, H., Fauzi, Y., & Bintara, H. (2017, January 5). Mengenal Confidentiality, Integrity, dan Availability Pada Keamanan Informasi. Retrieved from <https://netsec.id/confidentiality-integrity-availability-keamanan-informasi/>.
2. Pengertian Confidentiality,Integrity, Availability, Non repudiation, Authentication, Access control, Accountability. (2013, February 14). Retrieved from <https://harrisdv.wordpress.com/2013/02/14/pengertian-confidentialityintegrity-availability-non-repudiation-authentication-access-control-accountability/>.
3. Encikpaw. (1970, January 1). cocu 2. Retrieved from <http://eppcsystem.blogspot.com/2016/04/identify-computer-maintenance.html>.