GARIS PANDUAN KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

JABATAN PERANCANGAN BANDAR DAN DESA SEMENANJUNG MALAYSIA

Seksyen Teknologi Maklumat

Bahagian Khidmat Pengurusan

Versi 2.0

27 Januari 2015

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN
23 Disember 2009	1.0	JPICT JPBDSM Bil. 4/2009

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN	MUKA SURAT
23 Disember 2009	2.0	i. Kemaskini perkara 1 seperti berikut: dan dibaca bersama Dasar Keselamatan ICT Kementerian Kesejahteraan Bandar, Perumahan Dan Kerajaan Tempatan (KPKT) (GPKTMDK(ICT) Terdahulu: Jabatan, DIGUGURKAN: selaras dengan Pekeliling Am Bilangan 2 Tahun 2007 Kementerian Perumahan dan Kerajaan Tempatan (KPKT).)	1
		ii. Kemaskini perkara 3 seperti berikut: **3. KESELAMATAN MAKLUMAT** (GPKTMDK(ICT) Terdahulu: ICT)	2
		Kemaskini perkara 5.3 b) seperti berikut: Sila layari https://webmail.1govuc.gov.my/; (GPKTMDK(ICT) Terdahulu: Sila layari http://www.townplan.gov.my/mail;)	9
		Kemaskini perkara 5.3 d) seperti berikut: d) Memastikan kata laluan mengandungi **kombinasi 2 nombor, 1 huruf besar dan 1 simbol** dengan **minimum dua belas (12) aksara**; (GPKTMDK(ICT) Terdahulu: Memastikan kata laluan mengandungi **kombinasi nombor, huruf dan simbol** dengan **minimum lapan (8) aksara**;)	9

		Kemaskini perkara 5.3 e) seperti berikut: (GPKTMDK(ICT) Terdahulu: DIGUGURKAN : Membuat **penukaran kata laluan setiap 3 bulan** bagi tujuan keselamatan;)	9
		Kemaskini perkara 5.3 f) seperti berikut: e) penghantaran adalah **tidak melebihi 10MB** (GPKTMDK(ICT) Terdahulu: f) penghantaran adalah **tidak melebihi 20MB**)	9
		Kemaskini perkara 5.3 g) seperti berikut: f) kerap agar **saiz storan tidak melebihi 500MB** (GPKTMDK(ICT) Terdahulu: g) kerap agar **saiz storan tidak melebihi 1MB**)	9
		Kemaskini perkara 5.3 h) hingga n) seperti berikut: g) hingga m) (GPKTMDK(ICT) Terdahulu: h) hingga n))	9-10
		Kemaskini perkara 6 b) seperti berikut: perisian anti virus tersebut (contohnya http://www.pandasecurity.com/malaysia/). (GPKTMDK(ICT) Terdahulu: perisian anti virus tersebut (contohnya http://www.bitdefender.com))	10

		Kemaskini perkara 7 f) seperti berikut: **sekurang-kurangnya <u>dua belas (12)</u> aksara** (GPKTMDK(ICT) Terdahulu: **sekurang-kurangnya <u>lapan (8)</u> aksara**)	11
		Kemaskini perkara 7 h) seperti berikut: (GPKTMDK(ICT) Terdahulu: DIGUGURKAN : h) Menukar kata laluan tiga (3) bulan sekali. Bagi emel jabatan, pengguna akan diprompt secara automatik untuk membuat penukaran kata laluan setiap 90 hari)	12
		Kemaskini perkara 7 h) hingga j) seperti berikut: 7 h) hingga i) (GPKTMDK(ICT) Terdahulu: 7 h) hingga j))	12
		Kemaskini perkara 8 seperti berikut: **8. KESELAMATAN FIZIKAL <u>PERKAKASAN ICT</u>** (GPKTMDK(ICT) Terdahulu: **KESELAMATAN FIZIKAL <u>KOMPUTER PERIBADI DAN KOMPUTER RIBA</u>**)	12

		Kemaskini perkara 8 seperti berikut: Sebagai satu langkah bagi memastikan keselamatan perkakasan ICT berada di tahap maksima, pengguna hendaklah sentiasa (GPKTMDK(ICT) Terdahulu: DIGUGURKAN: Pengguna komputer peribadi dan riba Jabatan)	12
		Kemaskini perkara 8 h) seperti berikut: Komputer riba jika dibekalkan; (GPKTMDK(ICT) Terdahulu: Tiada. TAMBAHAN PERKARA)	13
		Kemaskini perkara 8 l) seperti berikut: **l) Konfigurasikan komputer**kepada ***sleeping mode*** jika digunakan secara berterusan; (GPKTMDK(ICT) Terdahulu: **Rehatkan komputer** jika digunakan secara berterusan)	13
		Kemaskini perkara 9 b) seperti berikut: (GPKTMDK(ICT) Terdahulu: DIGUGURKAN : Pegawai yang dibenarkan adalah pegawai Unit Rangkaian, Keselamatan ICT, Pusat Data dan Korporat)	14

		Kemaskini perkara 9 f) seperti berikut: di dalam lingkungan +-20°C dan (GPKTMDK(ICT) Terdahulu: di dalam lingkungan +-19.5°C dan)	15
		Kemaskini perkara 9 g) seperti berikut: diselenggarakan secara berkala; (GPKTMDK(ICT) Terdahulu: diselenggarakan sekerap yang mungkin;)	15
		Kemaskini perkara 9 i) seperti berikut: Reka letak perkakasan ICT hendaklah disediakan dan dipamerkan dalam Pusat Data (GPKTMDK(ICT) Terdahulu: DIGUGURKAN : Kertas cetakan yang tidak digunakan perlu diricih DIGANTI PERKARA)	15
		Kemaskini perkara 9 j) seperti berikut: Semua pergerakan keluar dan masuk pengguna di Pusat Data perlu direkod dalam buku log dan mendapat kebenaran STM (GPKTMDK(ICT) Terdahulu: TIADA . TAMBAHAN PERKARA)	15

		Kemaskini perkara 10 seperti berikut: Proses membaikpulih system terbahagi kepada dua peringkat iaitu prosedur Salinan pendua (*backup*) dan prosedur baik pulih (*restore*) (GPKTMDK(ICT) Terdahulu: TIADA. TAMBAHAN PERKARA)	15
		Kemaskini perkara 10 b) seperti berikut: di buat pada setiap bulan (GPKTMDK(ICT) Terdahulu: di buat pada setiap malam)	15
		Kemaskini perkara 10 f) seperti berikut: Lokasi off-site kedua – di Bahagian Teknologi Maklumat, Kementerian Kesejahteraan Bandar, Perumahan dan Kerajaan Tempatan, Aras 2 - 38, No. 51, Persiaran Perdana, Presint 4, 62100, Putrajaya, Malaysia. (GPKTMDK(ICT) Terdahulu: DIGUGURKAN: Lokasi off-site kedua – di bangunan lain yang berdekatan atau mana-mana Jabatan kerajaan lain yang berdekatan dan mempunyai kemudahan untuk menyimpan media backup DAN DI GANTI PERKARA)	16

		Kemaskini perkara 10.1 seperti berikut: Pelan Pemulihan Bencana (DRC) bagi jabatan di tempatkan di Strateq Data Centre Sdn. Bhd., GDC-2 Project Management Office, No 12, Jalan Bersatu13/4, 46200, Petaling Jaya, Selangor. (GPKTMDK(ICT) Terdahulu: DiGUGURKAN: Data-data kritikal disalin (backup) ke dalam pita dan disimpan di dalam pusat data, di samping itu pendua bagi data-data tersebut telah dihantar dan disimpan di KPKT sebagai salah satu pelan pemulihan bencana. Keadaan ini dilakukan bagi memastikan data-data kritikal masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal di pusat data, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebagainya DAN DIGANTI PERKARA)	16
		Kemaskini perkara 12 f) seperti berikut: Media storan **tidak melebihi ruang storan** yang diperuntukkan (GPKTMDK(ICT) Terdahulu: DIGUGURKAN : (1.44MB bagi disket))	18

		Kemaskini perkara 12 h) seperti berikut: **Elakkan**media storan dari terkena (GPKTMDK(ICT) Terdahulu: **Elakkan**disket dari terkena)	18
		Kemaskini perkara 12 j) seperti berikut: Sebarang media storan mestilah senantiasa di imbas sebelum di gunakan. (GPKTMDK(ICT) Terdahulu: TAMBAHAN PERKARA)	19

		Kemaskini perkara 13 seperti berikut: Sebarang kemusykilan atau pertanyaan berkaitan Garis Panduan Mengenai Keselamatan ini, sila hubungi Seksyen Teknologi Maklumat, Bahagian Khidmat Pengurusan. **En. Irman bin Ibrahim :** **03–2265 0705** **(irman.ibrahim@townplan.gov.my)** **Puan Nur Hanisah bt Nor Sham :** **03 – 2265 0707** **(nurhanisah@townplan.gov.my)** **En. Abdul Hadi bin Zainal Abidin:** **03–2265 0709** **(abdulhadi@townplan.gov.my)** (GPKTMDK(ICT) Terdahulu: Sebarang kemusykilan atau pertanyaan berkaitan Garis Panduan Mengenai Keselamatan ini, sila hubungi Unit Rangkaian, Keselamatan ICT, Pusat Data dan Korporat, Seksyen Teknologi Maklumat, Bahagian Khidmat Pengurusan. **Cik Ilyana bt. Ab Rahman : 03 - 2699 2190 (ilyana@townplan.gov.my)** **En. Mohd Nazri b. Omar : 03 – 2699 2205 (nazri.omar@townplan.gov.my)** **En. Irman b. Ibrahim : 03 – 2699 2177 (irman.ibrahim@townplan.gov.my)** **En. Mohd Azman b. Mohd Salleh : 03 – 2699 2241 (azman.salleh@townplan.gov.my)**	19

		Kemaskini perkara 14 seperti berikut: Garis Panduan keselamatan ICT JPBDSM perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pengguna. Maklumat penting JPBDSM perlu sentiasa di dalam keadaan boleh dipercayai dan boleh dicapai pada bila-bila masa tanpa sebarang keraguan. Garis Panduan ini akan di kemaskini dari masa ke semasa selaras dengan arus perkembangan teknologi maklumat dan komunikasi serta perundangan. (GPKTMDK(ICT) Terdahulu: Secara ringkasnya, keselamatan ICT JPBDSM perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pengguna. Aspek keselamatan ICT merupakan tanggungjawab bersama dan tidak hanya dikhususkan kepada satu pihak sahaja. Maklumat penting JPBDSM perlu sentiasa di dalam keadaan boleh dipercayai dan boleh dicapai pada bila-bila masa tanpa sebarang keraguan.)	20

Kandungan

GARIS PANDUAN KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)
JABATAN PERANCANGAN BANDAR DAN DESA
SEMENANJUNG MALAYSIA

1. PENGENALAN

Garis Panduan Keselamatan ICT Jabatan Perancangan Bandar dan Desa Semenanjung Malaysia (JPBDSM) merupakan lanjutan daripada dan dibaca bersama Dasar Keselamatan ICT Kementerian Kesejahteraan Bandar, Perumahan Dan Kerajaan Tempatan (KPKT) yang telah dikeluarkan.

Garis panduan ini yang dikeluarkan oleh Seksyen Teknologi Maklumat (STM), Bahagian Khidmat Pengurusan adalah berdasarkan kepada garis panduan dan pekeliling yang telah dikeluarkan oleh MAMPU. Pekeliling yang diguna pakai bagi keselamatan ICT sektor awam adalah Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi.

Keselamatan ICT berdasarkan pekeliling tersebut meliputi semua data, peralatan, perisian, rangkaian dan kemudahan ICT yang lain. Untuk memastikan maklumat dan data penting Jabatan bebas daripada sebarang ancaman, semua pengguna adalah disarankan untuk mematuhi garis panduan ini.

2. OBJEKTIF

Tujuan utama Garis Panduan Keselamatan ICT JPBDSM adalah sebagai panduan untuk pengguna demi menjamin kesinambungan urusan Kerajaan dengan meminimumkan kesan insiden keselamatan. Keselamatan ICT berkait rapat dengan perlindungan maklumat dan aset ICT. Ini kerana komponen peralatan dan perisian yang merupakan sebahagian daripada aset ICT Kerajaan adalah pelaburan besar yang perlu dilindungi. Begitu juga dengan maklumat yang tersimpan di dalam sistem ICT. Ia amat berharga kerana banyak sumber

yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangkamasa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat. Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT Kerajaan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan.

Justeru, garis panduan ini diwujudkan supaya menjadi panduan kepada para pengguna agar kesahihan, keutuhan dan kebolehsediaan maklumat yang berterusan sentiasa terjamin.

3. KESELAMATAN MAKLUMAT

Keselamatan merupakan proses yang berterusan dan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Ia meliputi:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses kepada hanya pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas. Garis panduan ini diharapkan dapat menjamin keselamatan maklumat JPBDSM dalam beberapa aspek berikut:

a) Kerahsiaan (*Confidentiality*)

Maklumat tidak boleh disebarkan dengan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran.

b) Integriti (*Integrity*)

Data dan maklumat hendaklah tepat, lengkap dikemaskini dan tidak berlaku sebarang manipulasi. Perubahan sebarang data dan maklumat hanya boleh dilakukan oleh pegawai yang telah diberikan kuasa untuk mengubah maklumat yang berkenaan.

c) Kesahihan (*Authenticity*)

Punca data dan maklumat hendaklah dari punca yang sah dan tanpa keraguan.

d) Tidak Boleh Disangkal

Data atau maklumat hendaklah dijamin ketepatan, kesahihannya dan tidak boleh disangkal.

e) Kebolehsediaan (*Availability*)

Data dan maklumat hendaklah sentiasa boleh dicapai pada bila-bila masa.

Penggunaan ICT di agensi kerajaan adalah tertakluk kepada arahan/garis panduan/pekeliling yang dikeluarkan dari semasa ke semasa untuk memperkemaskan jentera kerajaan. Penggunaan ICT juga secara amnya adalah tertakluk kepada undang-undang Kerajaan Malaysia antaranya Electronic Transaction Act 2003, Digital Signature Act 2007, Computer Crime Act 1997, Communications and Multimedia Act 1998, TeleMedicine Act 1997 dan Akta Aktiviti Kerajaan Elektronik 2007.

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan perkara tersebut. Pertimbangan untuk akses adalah berdasarkan

kategori maklumat seperti yang dinyatakan dalam perenggan 53 Arahan Keselamatan.

Semua aset ICT termasuk komputer peribadi dan komputer riba yang dibekalkan kepada pengguna JPBDSM adalah untuk kemudahan tugas harian dan merupakan aset mutlak Kerajaan yang boleh ditarik balik pada bila-bila masa jika didapati terdapat penyalahgunaan. Sebarang penyalahgunaan dan kehilangan aset disebabkan kecuaian pegawai akan dikenakan tindakan tata tertib. Sebarang kerosakan atau kegagalan fungsi peralatan ICT perlu dilaporkan melalui Borang Aduan Kerosakan Peralatan Jabatan seperti **Lampiran I**.

4. KESELAMATAN RANGKAIAN DAN INTERNET

Keselamatan rangkaian merupakan perkara utama dalam pengawalan aset ICT dari dicerobohi oleh pihak luar mahupun dalaman sesebuah organisasi. Keselamatan rangkaian komputer sesebuah organisasi bergantung kepada reka bentuk rangkaian yang betul dan kukuh. Langkah-langkah yang perlu dipertimbangkan adalah:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
e) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem;
f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JPBDSM;

g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;
h) Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPBDSM;
i) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JPBDSM hendaklah mendapat kebenaran ICTSO; dan
k) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.

Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan capaian kepada pelbagai maklumat yang terdiri daripada pelbagai bentuk dan format bagi tujuan penyelidikan, analisis, rujukan dan lain-lain. Penggunaan Internet secara tidak bertanggungjawab adalah satu tindakan yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, di samping melemahkan dan mengganggu sistem dan rangkaian ICT JPBDSM serta merosakkan imej perkhidmatan awam. Untuk menjamin keselamatan ICT JPBDSM pengguna adalah **DILARANG**:

a) Menggunakan kemudahan Internet untuk tujuan peribadi, aktiviti komersial dan politik;
b) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen (cetak rompak);
c) Menyedia, memuat naik, memuat turun, menyimpan dan menyebarkan sebarang bahan, teks ucapan, imej atau bahan berunsurkan lucah, jenayah, pernyataan fitnah atau hasutan dan bercorak penentangan;
d) Menggunakan kemudahan perbincangan awam atas talian seperti *newsgroup* dan *bulletin board* kecuali mendapat kebenaran dan kelulusan kandungan daripada Ketua Jabatan;

e) Memuat naik, memuat turun, menyimpan dan menggunakan perisian *peer-to-peer* (p2p) dan berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;

f) Memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepilan fail melebihi saiz 20MB yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer; dan

g) Menggunakan kemudahan modem peribadi untuk membuat capaian terus ke Internet.

Adalah diingatkan bahawa setiap maklumat yang dikongsi melambangkan imej Kerajaan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan. Sebarang bentuk pelanggaran larangan di atas adalah menyalahi undang-undang Kerajaan Malaysia dan boleh dikenakan tindakan.

5. KESELAMATAN MEL ELEKTRONIK (E-MEL)

E-mel merupakan satu cara perhubungan yang paling mudah dan murah di antara pengguna dengan pelbagai pihak. Pihak STM memandang serius mengenai aspek keselamatan perhubungan melalui e-mel di antara pegawai-pegawai JPBDSM, terutama yang melibatkan dokumen terperingkat. E-mel yang diperuntukkan oleh Jabatan hanya boleh digunakan untuk tujuan rasmi sahaja.

E-mel rasmi boleh dibahagikan kepada dua kategori berikut:

i. E-mel Rahsia Rasmi

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

ii. E-mel Bukan Rahsia Rasmi

E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi.

Semua pegawai JPBDSM adalah diperuntukkan satu akaun e-mel rasmi, walau bagaimanapun pewujudan akaun ini bukan secara automatik. Permohonan akaun emel baru perlu dibuat melalui Borang Pengurusan E-mel Rasmi Jabatan seperti di **Lampiran II**. Semua urusan *reset* kata laluan dan penutupan akaun juga perlu melalui borang ini. Pihak STM tidak akan melayan permohonan yang tidak menggunakan borang ini kecuali penutupan akaun boleh melalui makluman keluar / masuk kakitangan Jabatan. Penutupan akaun e-mel adalah dibuat seperti berikut:

i Akaun e-mel pengguna yang bersara dihapuskan serta merta;
ii Akaun e-mel pengguna yang bertukar ke Kementerian lain dihapuskan selepas sebulan pertukaran berkuatkuasa; dan
iii Akaun e-mel kakitangan yang bertukar ke OSC / JPBD Negeri / jawatan kader tidak ditutup tetapi ditangguh (*suspend*) selepas sebulan pertukaran berkuatkuasa. Pengguna boleh memohon untuk diaktifkan semula akaun tersebut.

Pengguna terbabit adalah dinasihatkan untuk membuat salinan emel yang perlu sebelum bertukar keluar / bersara (jika perlu).

5.1 Prosedur yang perlu dipatuhi

Bagi memastikan penggunaan e-mel dapat beroperasi dengan sempurna dan berkesan, pengguna adalah **DILARANG**:

a) Menggunakan kemudahan e-mel rasmi Jabatan untuk tujuan peribadi, aktiviti komersial dan politik;
b) Menggunakan akaun e-mel orang lain atau berkongsi e-mel atau memberi kata laluan akaun e-mel kepada orang lain;
c) Menghantar emel rasmi menggunakan akaun selain akaun emel rasmi Jabatan;
d) Membuka e-mel dari penghantar yang tidak dikenali yang berkemungkinan mengandungi virus;

e) Menyebarkan kod perosak seperti virus, *worm*, *Trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

f) Menyebarkan gambar-gambar lucah, e-mel berunsurkan fitnah, perkauman, gangguan seksual atau yang berkaitan dengannya;

g) Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya; dan

h) Membuka 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. Ia berkemungkinan akan menyebarkan virus apabila dibuka.

5.2 Pengendalian E-mel Rahsia Rasmi

Pengurusan maklumat terperingkat adalah tertakluk di bawah peruntukan Akta Rahsia Rasmi 1972. Perkara–perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan e-mel rahsia rasmi iaitu:

a) Maklumat terperingkat sebolehnya tidak di e-mel kecuali perlu;

b) Penyulitan mesti dilakukan ke atas semua e-mel rahsia rasmi yang dihantar, diterima dan disimpan;

c) Penerima e-mel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;

d) Penerima mesti membuat akuan penerimaan e-mel rahsia rasmi sebaik sahaja menerimanya;

e) E-mel rahsia rasmi bertanda Rahsia Besar dan Rahsia tidak boleh dimajukan kepada pihak lain. Sementara e-mel bertanda Sulit dan Terhad yang hendak dimajukan kepada pihak lain memerlukan izin daripada pemula dokumen; dan

f) E-mel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan perlulah dihapuskan secara kekal dari folder ‘Deleted Items’ atau dengan melaksanakan ‘Empty Trash’.

5.3 Tanggungjawab Pengguna

Pengguna hendaklah mematuhi tatacara penggunaan e-mel yang telah ditetapkan agar keselamatan ke atas penggunaannya terus terjamin. Peranan dan tanggungjawab pengguna adalah seperti berikut:

a) Tidak mendedahkan kata laluan kepada sesiapa walaupun diminta sama ada melalui e-mel atau medium lain;
b) Menggunakan webmail JPBDSM jika ingin membuat capaian e-mel rasmi Jabatan. Sila layari https://webmail.1govuc.gov.my/;
c) Membuat permohonan akaun e-mel baru, penutupan akaun emel sedia ada dan *reset* kata laluan menggunakan Borang Pengurusan E-mel Rasmi Jabatan seperti di **Lampiran II**;
d) Memastikan kata laluan mengandungi kombinasi 2 nombor, 1 huruf besar dan 1 simbol dengan minimum dua belas (12) aksara (Contoh: P@ssword&123);
e) Memastikan saiz fail kepilan (*attachment file*) termasuk kandungan e-mel yang dibenarkan untuk penghantaran adalah tidak melebihi 10MB;
f) Melakukan penyelenggaraan akaun dengan kerap agar saiz storan tidak melebihi 500MB. Penyelenggaraan boleh dilakukan dengan memadam atau menyalin mana-mana e-mel yang telah dibaca atau diambil tindakan. Ini bertujuan untuk menjamin prestasi server e-mel;
g) Mencetak dan mendokumenkan semua e-mel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada cakera keras komputer;
h) Membuat salinan dan menyimpan fail kepilan ke dalam satu *folder* berasingan daripada setiap e-mel yang penting bagi tujuan *backup* jika berlaku sebarang masalah kepada cakera keras komputer. Sila rujuk **Lampiran III**;
i) Melakukan imbasan ke atas semua fail dan fail kepilan bagi mengenal pasti fail yang diserang virus dengan perisian anti virus yang diguna pakai Jabatan;

j) Memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan segera dapat diambil ke atasnya;

k) Untuk keselamatan dokumen rahsia rasmi dan maklumat terperingkat yang dihantar melalui e-mel disulitkan terlebih dahulu;

l) Menggunakan *carbon copy* (cc) apabila e-mel tersebut perlu dimaklumkan kepada penerima lain. Sebolehnya penggunaan *blind carbon copy* (bcc) dielakkan kerana dilihat sebagai ingin menyembunyikan sesuatu; dan

m) Memaklumkan dengan segera nama kakitangan JPBDSM yang bertukar atau berhenti kepada STM agar akaun e-mel mereka dapat dikemaskini.

Pihak STM tidak akan bertanggungjawab ke atas e-mel yang hilang bagi pengguna yang tidak mematuhi polisi penggunaan e-mel.

6. KESELAMATAN DARI ANCAMAN VIRUS DAN *SPYWARE*

Serangan virus komputer dan *spyware* boleh menyebabkan kerosakan ke atas peralatan komputer, kehilangan atau kerosakan maklumat penting dan boleh disebarkan tanpa disedari oleh pengguna.

Untuk meningkatkan lagi tahap keselamatan maklumat dan infrastruktur ICT JPBDSM dari ancaman virus dan *spyware*, semua pengguna dikehendaki mengambil langkah-langkah keselamatan berikut:

a) Sentiasa melakukan imbasan dan nyah virus (*virus scanning*) ke atas setiap media storan luar (disket / cakera padat / external hard disk / pendrive dsb.) untuk mengesahkan bahawa ianya adalah bebas daripada sebarang virus atau *spyware*. Dengan cara ini, pengguna dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus;

b) Menggunakan perisian anti virus yang sah dan diperoleh oleh Jabatan. Maklumat terkini berkaitan serangan virus dan penyelesaian boleh didapati dengan melayari laman web perisian anti virus tersebut (contohnya http://www.pandasecurity.com/malaysia/).

c) Tidak melayari sebarang laman web berunsur lucah yang mana sudah diketahui umum mempunyai banyak *spyware* yang boleh menyebabkan penurunan prestasi komputer pengguna selain daripada boleh mencuri maklumat yang terkandung di dalam komputer pengguna;
d) Memastikan setiap komputer dan komputer riba yang digunakan dilakukan proses imbasan dan nyah virus sekerap yang mungkin. Ini bertujuan untuk memastikan bahawa semua komputer yang digunakan adalah bebas daripada sebarang virus; dan
e) Memaklumkan serangan virus dan *spyware* kepada STM supaya tindakan lanjut dapat diambil.

7. KESELAMATAN ID PENGGUNA DAN KATA LALUAN (*PASSWORD*)

ID pengguna dan kata laluan merupakan kata kunci atau *pin number* yang menjadi hak individu dan menjadi rahsia dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga ID pengguna dan kata laluan masing-masing dengan teliti agar tidak dicerobohi oleh pengguna lain. Bagi menjamin keselamatan ID pengguna dan kata laluan, pengguna hendaklah mengambil langkah-langkah keselamatan berikut:

a) ID pengguna yang diberikan bagi setiap sistem aplikasi adalah unik bagi setiap pengguna dan akan menggunakan sama ada nombor kad pengenalan pengguna atau nama pengguna;
b) ID pengguna dan kata laluan bagi satu-satu sistem aplikasi tidak dibenarkan sama;
c) Aplikasi sebolehnya mempunyai ciri log keluar automatik selepas masa tidak aktif (contohnya selepas 15 minit);
d) Rahsiakan ID pengguna dan kata laluan. ID pengguna dan kata laluan hendaklah dihafal dan tidak disalin atau disimpan di dalam mana-mana media seperti buku catatan, disket, CD dan sebagainya kerana dikhuatiri akan diketahui dan disalah gunakan oleh mereka yang tidak bertanggungjawab;
e) Menggunakan kata laluan berbeza daripada ID pengguna;
f) Menggunakan kata laluan sekurang-kurangnya dua belas (12) aksara;

g) Menggunakan kata laluan yang kukuh dengan kombinasi nombor, huruf dan simbol (*contoh: P@ssword&123*);
h) Melaporkan kepada pegawai keselamatan ICT (ICTSO) Jabatan sekiranya kata laluan telah dicerobohi atau disyaki telah dicerobohi. Kata laluan sedia ada akan diubah serta merta; dan
i) ID pengguna dan kata laluan bagi sistem aplikasi Jabatan akan ditarik balik serta merta setelah pengguna bertukar/bersara.

Sila rujuk **Lampiran IV** untuk mengetahui cara-cara untuk mengubah kata laluan e-mel dan Sistem FirdausNet.

8. KESELAMATAN FIZIKAL PERKAKASAN ICT

Keselamatan fizikal meliputi komputer peribadi, komputer riba dan perkakasan terlibat seperti cakera keras, pencetak, pengimbas dan lain-lain. Sebagai satu langkah bagi memastikan keselamatan perkakasan ICT berada di tahap maksima, pengguna hendaklah sentiasa mematuhi peraturan keselamatan berikut:

a) Setiap komputer mestilah mempunyai kata laluan;
b) Pengguna dinasihatkan supaya membuat *backup* semua dokumen dan data penting yang disimpan di cakera keras (*hard disk*) komputer ke media storan lain secara berkala sekerap mungkin bagi langkah pemulihan sekiranya berlaku kerosakan;
c) Pengemaskinian *Microsoft Windows, patches* dan *service pack* yang terkini mestilah dilakukan ke atas setiap komputer dari semasa ke semasa. Sila hubungi STM untuk bantuan;
d) Setiap komputer mestilah mempunyai perisian anti virus yang diguna pakai di Jabatan;
e) Pengguna dilarang sama sekali mengubah atau meminda "*Computer Name*" dan "*Description*" di dalam komputer;
f) Jangan biarkan komputer berada di atas talian (*on-line*) jika tidak digunakan, dan *log off* komputer sebelum meninggalkan pejabat;

g) Pastikan komputer pejabat hanya digunakan untuk urusan pejabat sahaja dan tidak digunakan oleh orang lain yang tidak berkenaan;

h) Dilarang menggunakan alat penyambung kuasa elektrik bagi pelbagai peralatan. Bekalan kuasa elektrik yang tidak stabil akan merosakkan komputer. Gunakan kemudahan *Uninterruptible Power Supply (UPS*) atau *Automatic Voltage Regulator (AVR)* untuk memastikan bekalan elektrik sentiasa dibekalkan mengikut spesifikasi keperluan komputer atau komputer riba jika dibekalkan;

i) Pastikan bekalan atau punca elektrik ditutup semasa pemasangan atau penyambungan peralatan komputer dan aksesorinya atau setelah selesai menggunakan komputer;

j) Pastikan komputer tidak terdedah secara terus kepada pancaran matahari/haba dan elakkan komputer daripada kawasan tarikan kuasa magnet/kuasa voltan yang tinggi;

k) Pastikan komputer diletakkan di tempat dingin dan kering persekitarannya serta di tempat yang selamat;

l) Konfigurasikan computer kepada *sleeping mode* jika digunakan secara berterusan;

m) Tamatkan "*not responding*" dengan menekan kekunci *Ctrl-Alt-Del* jika sebarang program komputer tidak berfungsi (*hang*);

n) Pastikan komputer mempunyai *system date & time* yang betul untuk tujuan audit dan penghantaran e-mel;

o) Sentiasa keluar dari Windows atau menutup komputer dengan cara yang betul bagi mencegah ralat sistem iaitu klik *Start -> Shut Down*. DILARANG sama sekali menutup komputer secara fizikal iaitu dengan menutup suis atau mencabut *plug* atau sebagainya;

p) DILARANG menghentak/mengetuk dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer;

q) Pastikan komputer riba disimpan di dalam almari berkunci setelah digunakan;

r) Pengguna dinasihatkan membuat *basic maintenance* seperti *clean up*, *defragmentation* dan *scan disk* secara berkala setiap bulan seperti di **Lampiran V**; dan

s) Tidak dibenarkan membaiki sendiri komputer jika terdapat sebarang masalah atau kerosakan. Sila hubungi STM untuk bantuan.

Sebarang kehilangan dan apa juga bentuk penyalahgunaan penggunaan aset ICT Kerajaan terutama komputer boleh dikenakan tindakan, dan kemudahan boleh ditarik balik pada bila-bila masa.

8.1 Kemudahan komputer di bilik mesyuarat dan makmal komputer

Pengguna perlu mematuhi peraturan penggunaan seperti berikut:

a) Membuat permohonan secara rasmi kepada Ketua STM bagi penggunaan makmal komputer;
b) Memadamkan dokumen yang disimpan di dalam komputer selepas selesai digunakan;
c) Tidak membuat sebarang instalasi perisian kepada komputer kecuali dengan kebenaran STM; dan
d) Memastikan komputer di *shut down* dan semua suis dimatikan selepas tamat penggunaan.

9. KESELAMATAN PUSAT DATA

Untuk memastikan server penting sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa, semua *server* hendaklah diletakkan di dalam Pusat Data yang mempunyai kemudahan keselamatan, penyaman udara khas, dan kemudahan perlindungan suhu dan kebakaran. Pusat Data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti firewall dan UPS. Antara langkah yang boleh dilaksanakan bagi melindungi Pusat Data ialah:

a) Dilengkapi pintu akses yang kukuh;
b) Hanya pegawai STM yang mempunyai akses sahaja yang dibenarkan masuk;
c) Pengguna lain / pihak ketiga perlu memohon kebenaran masuk ke Pusat Data dari Ketua STM dan diiringi pegawai STM pada setiap masa;

d) Setiap server mestilah dilabelkan penggunaannya bagi memudahkan pentadbir menjalankan tugas;
e) Pastikan Pusat Data sentiasa bersih dan server serta peralatan lain tidak terdedah kepada habuk;
f) Penghawa dingin mestilah berfungsi dengan baik di mana suhu di dalam lingkungan +-20°C dan kelembapan di paras 50.7%;
g) Semua peralatan keselamatan, UPS dan penghawa dingin mestilah diselenggarakan secara berkala;
h) Alat pemadam kebakaran perlu diletakkan di tempat yang mudah diakses;
i) Reka letak perkakasan ICT hendaklah disediakan dan dipamerkan dalam Pusat Data; dan
j) Semua pergerakan keluar dan masuk pengguna di Pusat Data perlu direkod dalam buku log dan mendapat kebenaran STM.

10. KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA

Data dan maklumat sistem aplikasi yang telah dibangunkan dan beroperasi merupakan aset yang penting dan perlu dilindungi sebaik mungkin demi menjamin keselamatannya.

Antara langkah yang telah dikenalpasti dan dilaksanakan bagi melindungi perisian sistem dan pangkalan data adalah proses *backup* dan *restore*. Proses ini dibuat sekiranya perkara berikut berlaku:

a) Kegagalan server berfungsi
b) Kerosakan fizikal cakera keras
c) Masalah dalam pemprograman

Proses membaikpulih sistem terbahagi kepada dua peringkat iaitu prosedur Salinan pendua (*backup*) dan prosedur baik pulih (*restore*). Perkara yang perlu dipatuhi bagi Salinan pendua (*backup*) ialah:

a) *Backup file* perlu dilabel dengan betul agar tidak berlaku kesalahan pemadaman;
b) *Backup* keseluruhan data dan aplikasi dibuat pada setiap bulan untuk semua server berpandukan prosedur *backup* yang telah ditetapkan;

c) *Backup* atau salinan data ke dalam media storan perlu dilakukan setiap hari untuk mengelakkan kehilangan data sekiranya berlaku kerosakan cakera keras;

d) Pelabelan nama fail yang disalin (*backup*) untuk memudahkan carian fail dari masa ke semasa;

e) *Backup* sistem aplikasi perlu dibuat sekurang-kurangnya sekali bagi setiap keluaran versi terbaru dari masa ke semasa mengikut peraturan yang ditetapkan semasa perisian itu dibangunkan atau diperolehi atau mengikut garis panduan yang dikeluarkan dari masa ke semasa. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam menentukan kekerapan *backup*.

f) *Backup* untuk data dan sistem aplikasi dicadangkan dibuat dalam tiga (3) salinan dan setiap satu disimpan di lokasi yang berlainan. Lokasi tersebut adalah:

- Lokasi di mana sistem tersebut beroperasi
- Lokasi *off-site* pertama – di Seksyen Teknologi Maklumat
- Lokasi *off-site* kedua – di Bahagian Teknologi Maklumat, Kementerian Kesejahteraan Bandar, Perumahan dan Kerajaan Tempatan Aras 2 - 38, No. 51, Persiaran Perdana, Presint 4, 62100, Putrajaya, Malaysia.

Penetapan lokasi simpanan *backup* ini adalah untuk memastikan data-data kritikal/penting masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal, contohnya jika berlaku bencana seperti kebakaran, banjir dan sebagainya.

10.1 Pelan Pemulihan Bencana

Pelan Pemulihan Bencana (DRC) bagi jabatan ditempatkan di Strateq Data Centre Sdn. Bhd., GDC-2 Project Management Office, No 12, Jalan Bersatu13/4, 46200, Petaling Jaya, Selangor.

11. TATACARA PEMINJAMAN PERALATAN ICT

Pendaftaran aset ICT buat masa ini adalah di bawah setiap Bahagian. Oleh itu setiap Bahagian adalah bertanggungjawab memastikan supaya segala peralatan ICT termasuk projektor, komputer riba, komputer, pencetak dan aksesori yang berkaitan seperti *plug extension*, kabel komputer dan sebagainya yang dipinjam atau dibawa keluar atau masuk daripada premis pemunya (contohnya peralatan pinjaman STM) adalah tertakluk di bawah prosedur berikut:

a) Semua pinjaman peralatan ICT perlu melalui permohonan rasmi secara memo atau emel kepada Pengarah Bahagian / Ketua Seksyen pemunya;
b) Setiap pengguna dikehendaki mengisi dan menandatangani Borang Peminjaman Peralatan ICT seperti **Lampiran VI** dan KEW. PA-6;
c) Peralatan ICT yang dipinjam dan borang tersebut perlu dikembalikan setelah selesai menggunakannya untuk semakan dan simpanan pihak pemunya;
d) Adalah menjadi tanggungjawab peminjam untuk:

- menjaga dengan baik peralatan ICT agar tidak berlaku kerosakan atau kehilangan;
- memastikan kesemua peralatan ICT dikembalikan dengan sempurna, lengkap dan selamat;
- memastikan semua dokumen yang disimpan di dalam *hard disk* komputer riba yang dipinjam dipindahkan ke storan lain sebelum dipulangkan, dan dipadam daripada *hard disk* komputer riba yang dipinjam sebelum dipulangkan. Pihak STM akan membuat *housekeeping* ke atas semua komputer riba pinjaman dan tidak akan bertanggungjawab sekiranya peminjam gagal memindahkan dokumen ke storan lain;
- memastikan semua media storan elektronik luar (disket / pen drive / external hard disk dsb.) yang disambung ke komputer riba pinjaman dinyah virus (*scan*) terlebih dahulu sebelum dibuka;
- melaporkan sebarang kerosakan dan kegagalan peralatan ICT kepada STM dengan segera melalui Borang Aduan Kerosakan Peralatan Jabatan; dan

- melaporkan sebarang kehilangan peralatan ICT yang dipinjam kepada pemunya dengan segera supaya tindakan yang berkaitan dapat diambil.

12. TATACARA PENGURUSAN MEDIA STORAN

Disket / CD / pen drive merupakan antara media storan elektronik luar yang digunakan untuk menyimpan data atau kandungan fail. Untuk menjamin keselamatan kandungan, pengguna adalah dinasihatkan supaya mengikuti langkah-langkah berikut:

a) Media storan yang diperolehi adalah untuk tujuan rasmi sahaja;
b) Setiap media storan perlulah dilabelkan mengikut Bahagian/Unit/Nama;
c) Setiap pen drive juga perlulah dilabelkan (*volume label*) untuk memudahkan pengecaman hakmilik. Sila rujuk **Lampiran VII** untuk cara pelabelan;
d) Media storan yang mengandungi maklumat sulit/ rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad atau Sulit dan mestilah disimpan di tempat yang selamat. Bagi fail yang diklasifikasikan sebagai Rahsia/Sulit, pengguna dinasihatkan untuk mewujudkan kata laluan bagi fail-fail tersebut. Cara-cara untuk mewujudkan kata laluan boleh didapati di **Lampiran VIII** ;
e) Pengguna adalah DILARANG membawa keluar atau memberi media storan yang mengandungi maklumat rahsia rasmi kepada orang lain. Ini adalah untuk mengelakkan daripada berlakunya kebocoran rahsia;
f) Pengguna hendaklah memastikan saiz fail yang disimpan di dalam media storan tidak melebihi ruang storan yang diperuntukkan dan mengutamakan penyimpanan fail yang perlu sahaja. Sekiranya perlu disarankan untuk melakukan kaedah pemampatan (*compress*) untuk mengurangkan saiz fail;
g) Media storan yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadam (*delete*) sebelum digunakan untuk tujuan yang lain;
h) Elakkan media storan dari terkena debu atau habuk, sinaran matahari, suhu panas, elektrostatik dan magnet serta disimpan di tempat yang selamat. Ini dapat mengelakkan maklumat atau data menjadi rosak (*corrupted*) atau tidak boleh dibaca. Bagi penggunaan pen drive, ia mestilah dikeluarkan

daripada sistem dengan cara yang betul. Pengguna dilarang mengeluarkan pen drive dari USB dengan terus. Sila rujuk **Lampiran IX**;

i) Sekiranya media storan yang digunakan adalah yang telah lama jangka hayatnya, kandungan fail atau maklumat di dalamnya perlulah dipindahkan ke media lain seperti CD, pen drive dan lain-lain media storan; dan

j) Sebarang media storan mestilah senantiasa diimbas sebelum digunakan.

12.1 Pemusnahan Media Storan

Kaedah pemusnahan media adalah seperti berikut:

a) Media magnetik

i. Mendedahkan media kepada medan magnet yang kuat.

ii. Format semula bagi memadamkan semua data dan diguna pakai semula.

b) Media optik

i. Kaedah pemusnahan secara fizikal iaitu memotong, menggunting dsb.

ii. Format semula *rewritable optical disk* bagi memadamkan semua data dan diguna pakai semula.

13. KHIDMAT NASIHAT

Sebarang kemusykilan atau pertanyaan berkaitan Garis Panduan Mengenai Keselamatan ini, sila hubungi Seksyen Teknologi Maklumat, Bahagian Khidmat Pengurusan.

En. Irman bin Ibrahim : 03-2265 0705
(irman.ibrahim@townplan.gov.my)
Puan Nur Hanisah bt Nor Sham : 03-2265 0707
(nurhanisah@townplan.gov.my)
En. Abdul Hadi bin Zainal Abidin: 03-2265 0709
(abdulhadi@townplan.gov.my)

14. PENUTUP

Garis Panduan Keselamatan ICT JPBDSM perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pengguna. Maklumat penting JPBDSM perlu sentiasai dalam keadaan boleh dipercayai dan boleh dicapai pada bila-bila masa tanpa sebarang keraguan. Garis Panduan ini akan dikemaskini dari masa ke semasa selaras dengan pekeliling dan mengikut keperluan.

Lampiran I

	PENGURUSAN ASET MELIPUTI PENYELENGGARAAN DAN PELUPUSAN	NO. KELUARAN: 1	MUKA SURAT: 19 DARI 27
	JPBD(IP) PKT 08	NO. PINDAAN: 0	TARIKH: 8 Oktober 2009

Lampiran 5

A. ADUAN KEROSAKAN

TARIKH :

MASA :

PENGADU :

BAHAGIAN/SEKSYEN :

NO TEL :

PENERIMA ADUAN :

BUTIRAN PERALATAN YANG ROSAK

JENIS:	KOMP. DESKTOP / KOMP. RIBA / MONITOR / PENCETAK / PENGIMBAS / PLOTTER / PERISIAN
MODEL :	HP / DELL / ACER / IBM / EPSON / LEXMARK / .....
LOKASI :	
NO. SIRI PENDAFTARAN ASET (SPA):	KPKT / JPBD / / H / /
MAKLUMAT KEROSAKAN :	
STATUS :	☐ DALAM WARANTI ☐ TAMAT WARANTI

B. TINDAKAN YANG DIAMBIL (SILA CATATKAN TARIKH DAN BUTIRAN TINDAKAN)

C. PENGESAHAN PEGAWAI BAGI ADUAN YANG TELAH SELESAI

PEGAWAI STM YANG BERTANGGUNGJAWAB

NAMA:
TARIKH:

PEGAWAI BAHAGIAN YANG BERTANGGUNGJAWAB

NAMA:
TARIKH:

D. * HANYA DI ISI JIKA TINDAKAN MELIBATKAN PERALATAN YANG ROSAK DIBAWA KELUAR

NAMA PEGAWAI / SYARIKAT PEMBEKAL :

NO. TEL :

TARIKH :

SEBELUM DIBAWA KELUAR

PENGESAHAN PENYERAHAN

NAMA:
TARIKH:

PENGESAHAN PENERIMAAN

NAMA:
TARIKH:

SELEPAS SELESAI DIBAIKI

PENGESAHAN PENYERAHAN

NAMA:
TARIKH:

PENGESAHAN PENERIMAAN

NAMA:
TARIKH:

MS ISO 9001:2008

Lampiran II

BORANG PENGURUSAN EMEL

A. MAKLUMAT PERMOHONAN (DIISI OLEH PEMOHON)

1) Nama : 2) No. Kad Pengenalan :

3) Jawatan dan Gred :

4) Bahagian & Unit :

5) No. Tel. Pej. / HP : 6) No. Faks :

7) Jenis Permohonan : (Sila tandakan (X) yang berkenaan)

- ☐ Permohonan Baru
- ☐ Hapus (Sebab : _____)
- ☐ Reset password

(Sebab : _____)

8) Saya dengan ini mengesahkan bahawa kesemua maklumat yang diberi adalah benar. Saya berjanji akan menggunakan emel Jabatan mengikut yang digariskan PKPA Bil. 1Tahun 2003 (bagi permohonan baru)

T/tangan Pemohon : _____ Nama dan cop jawatan :

Tarikh : _____

B. MAKLUMAT PELAKSANAAN (DIISI OLEH STM)

Permohonan :

- ☐ Diluluskan
- ☐ Ditolak (Sebab : _____)

Alamat emel yang diwujudkan :

Kata laluan sementara ;

Pentadbir Emel : Tarikh : _____

Peringatan :

1. Penggunaan emel Jabatan adalah tertakluk di bawah Pekeliling Kemajuan Perkhidmatan Awam Bilangan 1 Tahun 2003 dan Dasar Keselamatan ICT Jabatan.
2. Emel yang disediakan hendaklah digunakan untuk tujuan rasmi sahaja.
3. Menggunakan emel Jabatan bukan untuk tujuan lain seperti menyedia dan menghantar maklumat berulang-ulang yang berupa gangguan, menyedia, memuat naik, memuat turun dan menyimpan maklumat yang mengandungi unsur-unsur lucah atau sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan, atau menggunakan emel untuk tujuan komersial, politik, perjudian dsb.
4. Kegagalan mematuhi kepada perkara tersebut di atas membolehkan Tuan/Puan diambil tindakan.

Lampiran III

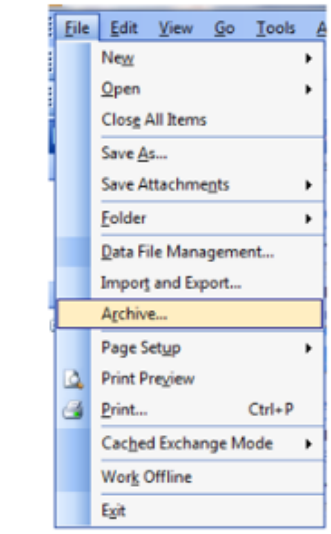
A. BACKUP DATA EMEL

MEMBUAT E-MEL ARKIB BAGI OUTLOOK 2003/2007/2010

Langkah 1

Arkib secara manual

1. Buka aplikasi Outlook 2003/2007/2010.
2. Cari tetingkap **Archive**.
3. Bagi Outlook 2003/2007:
   - Klik pada tab **File** dan kemudian pilih **Archive**.

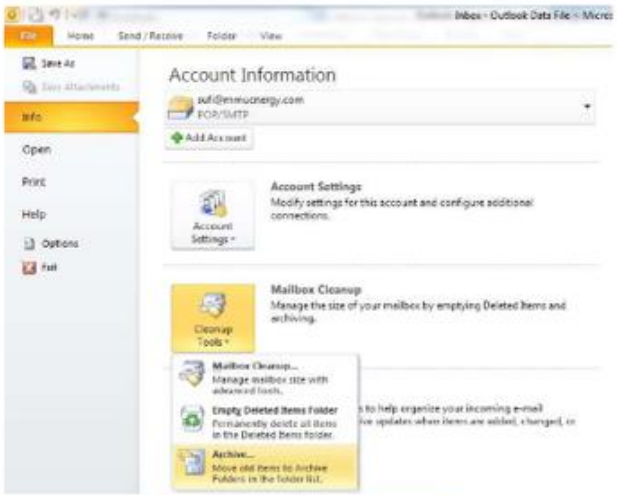


Outlook 2003/2007

Langkah 2

Bagi Outlook 2010:

- Klik pada tab **File**. Di bahagian tab **Cleanup Tools**, klik pada **Archive**.



Outlook 2010

Langkah 3

1. Pilih butang radio **Archive this folder and all subfolders**.
2. Pilih folder yang ingin diarkibkan.
3. Klik kotak **Include items with 'Do not AutoArchive' checked**.

Outlook 2003/2007/2010

Langkah 4

1. Di bahagian **Archive items older than**, pilih tarikh pada sebelum berlakunya arkib.
2. Klik **Browse** dan pilih lokasi untuk penyimpanan fail arkib.
   - Pada bahagian **File Name**, isikan nama bagi fail yang diarkib.
   - Kemudian klik **OK**.

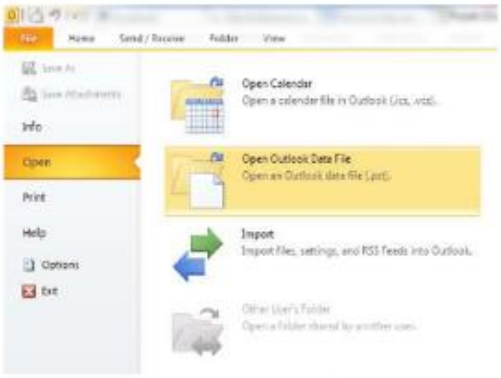
Outlook 2003/2007/2010

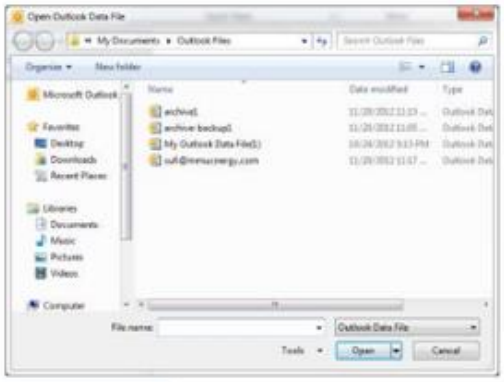
B. RESTORE DATA EMEL

MENGEMBALIKAN FAIL BACKUP / ARKIB (.PST) PADA OUTLOOK 2010

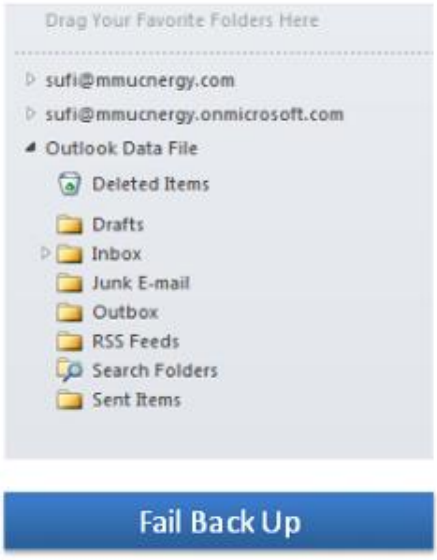
LANGKAH 1

1. Buka aplikasi Outlook 2010.
2. Klik pada tab **File**. Pilih **Open** dan kemudian klik pada **Open Outlook Data File**.
3. Pilih fail backup / arkib untuk dimasukkan dan klik **Open**.
4. Pastikan fail backup / arkib yang dimasukkan berada pada senarai **Navigation Pane**.

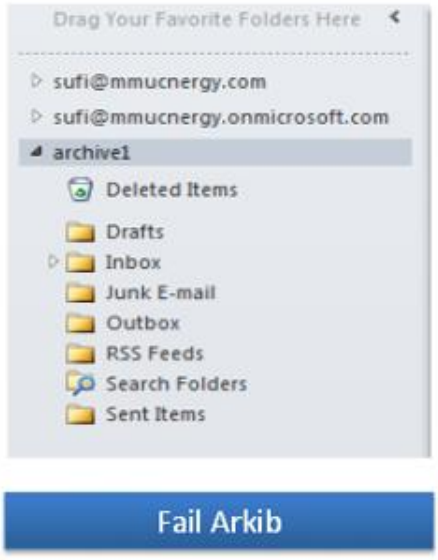




LANGKAH 2



Fail Back Up



Fail Arkib

Lampiran IV

A: PENUKARAN KATA LALUAN E-MEL

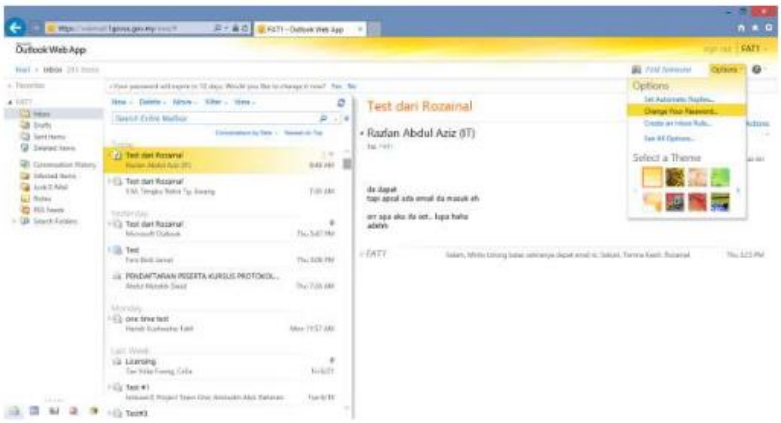
LANGKAH DEMI LANGKAH MENUKAR KATA LALUAN

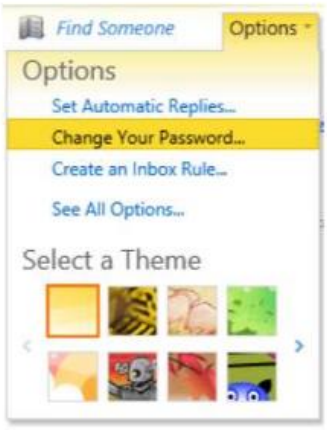
1. Berikut adalah polisi untuk katalaluan bagi pengguna 1GovUC

Polisi	Tetapan
Kuatkuasa sejarah katalaluan	4 sejarah kataluan
Maksimum umur katalaluan	90 hari
Minimum umur katalaluan	0 hari
Minimum panjang katalaluan	12 aksara
Katalaluan harus menepati kerumitan (complexity)	Dimestikan
Mempunya Aksara daripada kategori berikut	1. Huruf besar 2. Huruf kecil 3. Nombor (0 -9) 4. Simbol (contoh : !, @, #, $, %, &)

LANGKAH 1

1. Pertukaran katalaluan dilakukan pada pilihan *Options* di laman **Outlook Web App (OWA).**
2. Sila pilih pilihan Change Your Password





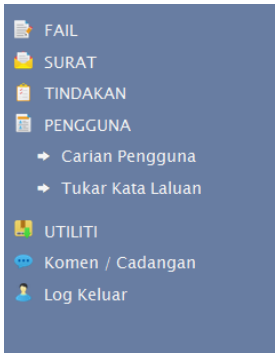
LANGKAH 2

1. Masukkan katalaluan lama di ruangan *Current Password*
2. Masukkan katalaluan di ruangan *New Password* dan *Confirm New Password*
3. Tekan butang *Save*

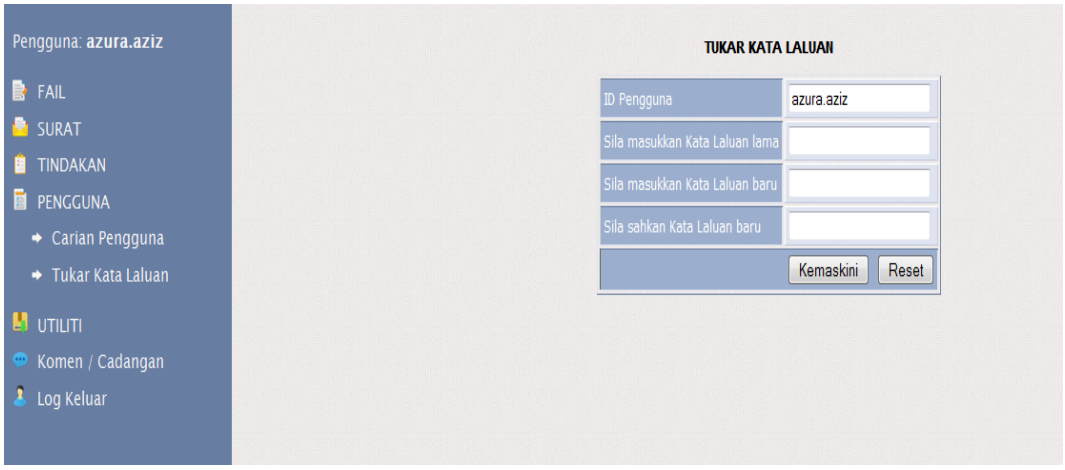
B: PENUKARAN KATA LALUAN FIRDAUSNET

LANGKAH 1

Klik pada Tukar Kata Laluan



Akan Pamerkan seperti berikut:



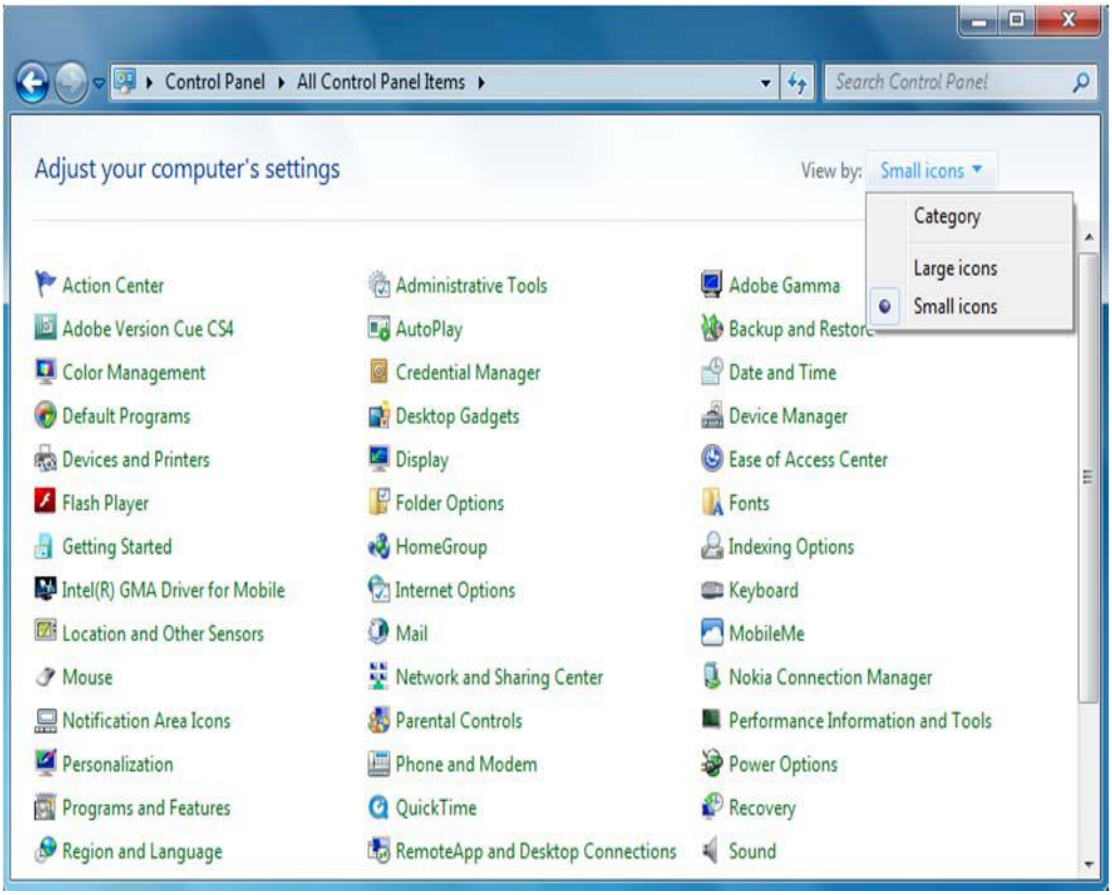
Lampiran IV

PENJAGAAN KOMPUTER SECARA ASAS BAGI SISTEM PENGOPERASIAN WINDOWS® 7

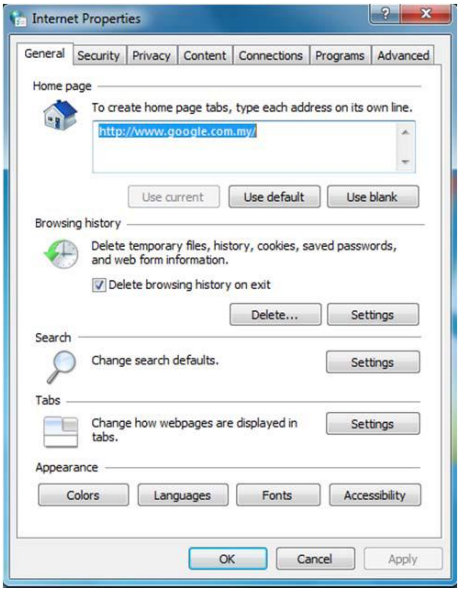
1. Tatacara Untuk *Delete Browsing History*.

i) Klik icon  pada *desktop* dan klik ***Control Panel.***

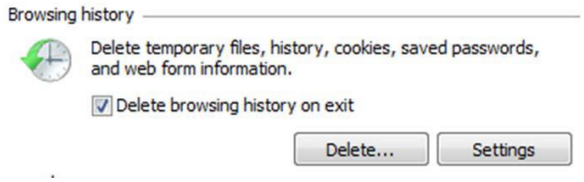
Nota:
Pada *Control Panel*, untuk *standard*kan kaedah carian, sila pilih ***View by: Large icons / Small icons*** dan skrin di bawah akan dipaparkan:-



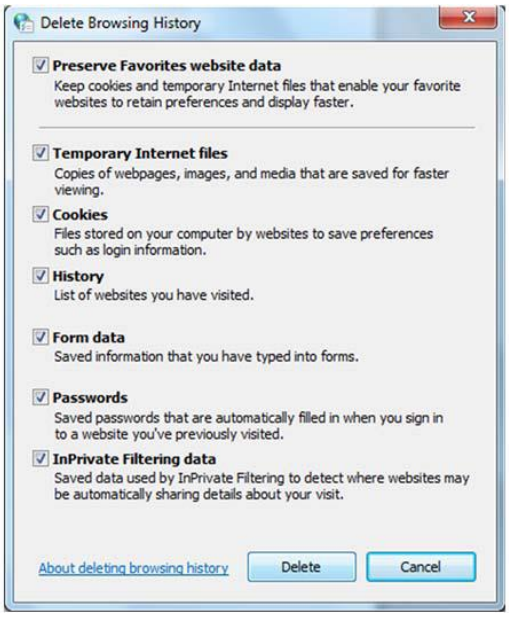
ii) Pilih ***Internet Options*** dan skrin *Internet Properties* berikut akan dipaparkan.



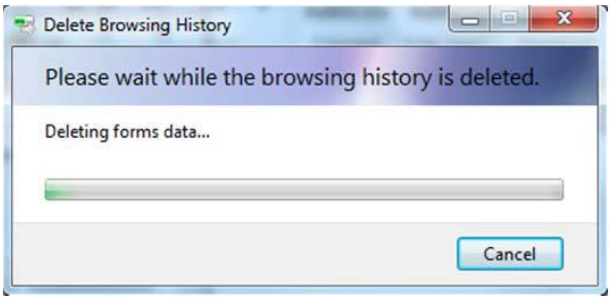
iii) Di bawah tajuk *Browsing history*, sila pastikan ***checkbox*** pada *Delete browsing history on exit* ditanda dengan √ dan klik butang **Delete...**



i) Setelah klik butang **Delete...**, skrin ***Delete Browser History*** akan dipaparkan. Pilih yang berkaitan untuk dibuang. Klik butang ***Delete***.



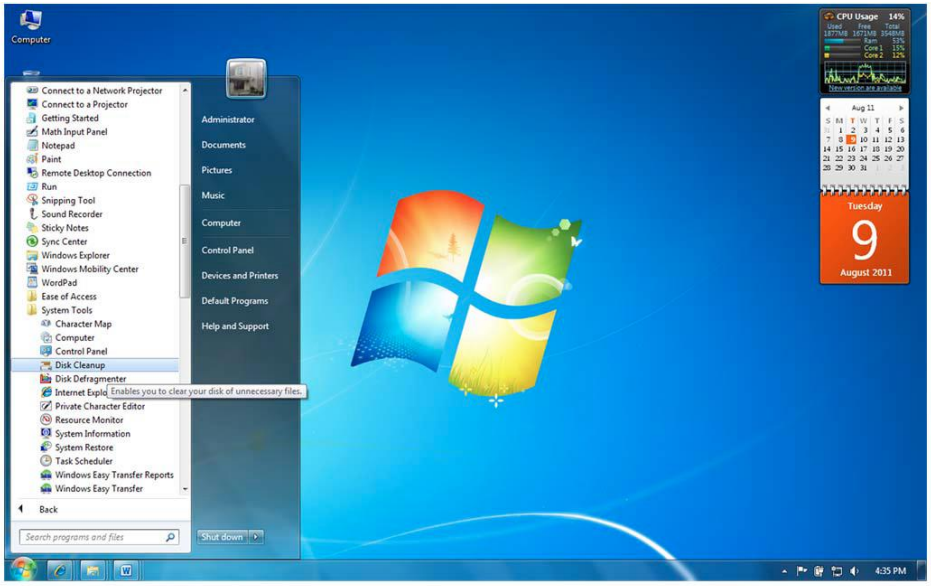
ii) Tunggu sehingga proses selesai.



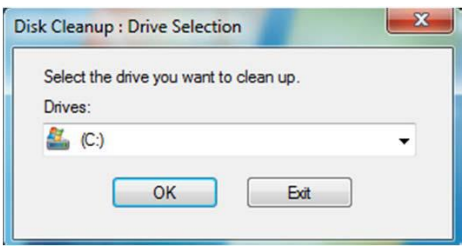
iii) Proses tamat.

2. *Disk Cleanup.*

i) Klik icon  pada *desktop* >***All Programs*** >***Accessories*** >***System Tools*** >***Disk Cleanup***



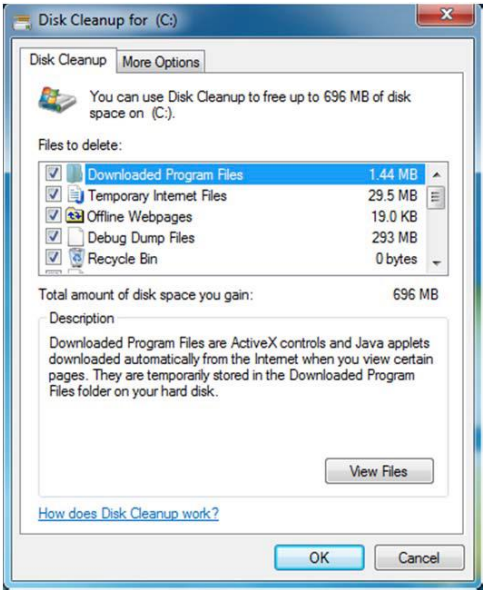
ii) Apabila skrin di bawah dipaparkan, sila pilih ***Drive*** sebagai contoh (C:) dan klik butang ***OK*.**



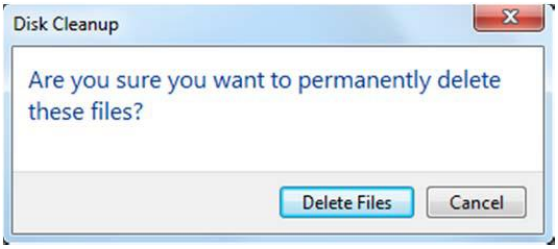
iii) Apabila skrin *Disk Cleanup for* (C:) dipaparkan, sila pilih *file* yang hendak di *delete* seperti *Download Program Files*, *Temporary Internet Files*, *Recycle Bin*, *Temporary Files* dan *Thumbnails*.

Nota:

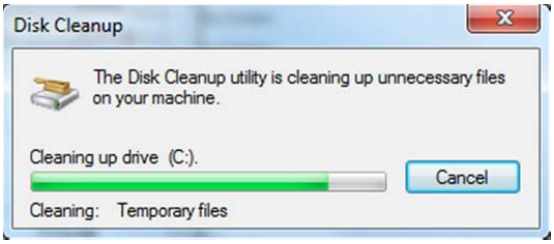
Digalakkan pengguna untuk memilih semua fail yang disenaraikan untuk dibuang



iv) Klik butang ***OK*** dan apabila skrin di bawah dipaparkan, klik butang ***Delete Files***.



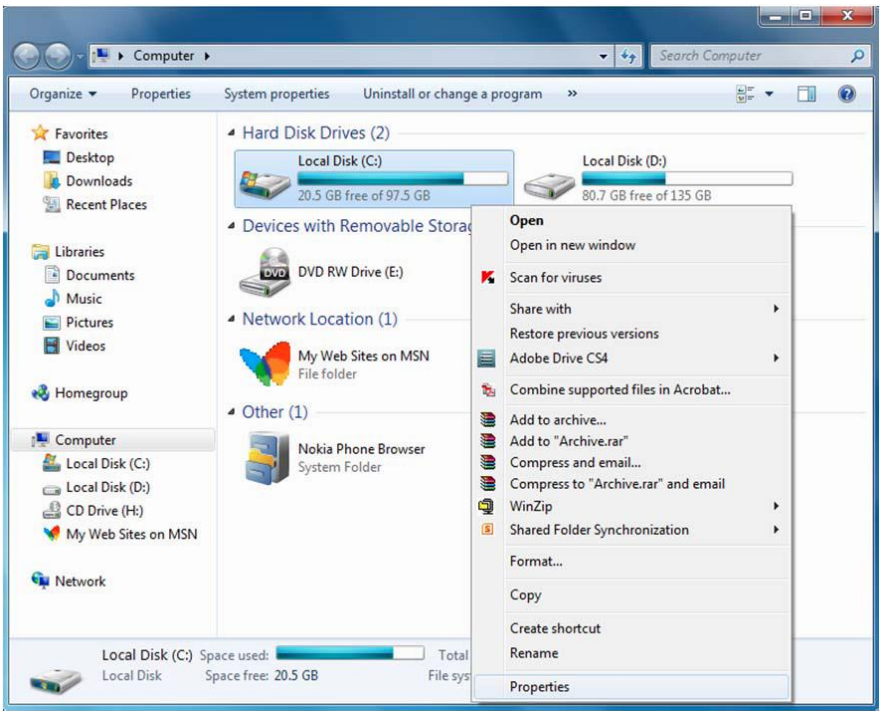
v) Tunggu sehingga proses selesai



vi) Proses tamat.

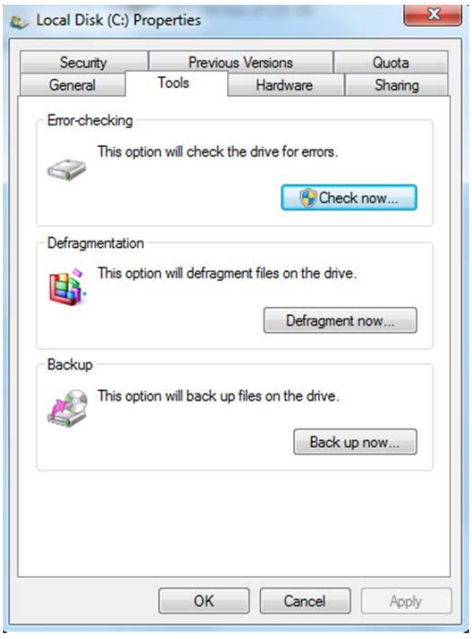
3. *Error checking*

i) Pada skrin *desktop*, klik dua kali pada ikon dan skrin berikut akan dipaparkan.

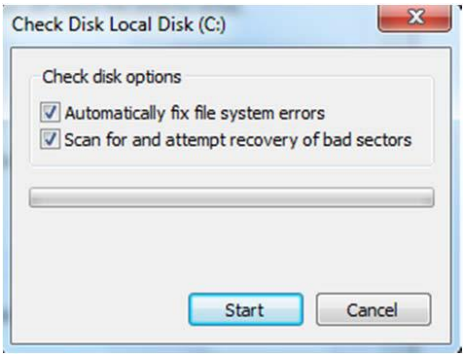


ii) Klik kanan pada *Local Disk (C:)* dan pilih ***Properties***. Apabila skrin *Local Disk (C:)*

Properties dipaparkan, pilih Tab ***Tools*** seperti skrin di bawah:-



iii) Klik butang ***Check now*** dan skrin berikut dipaparkan.

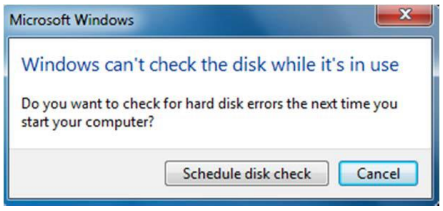


iv) Tandakan√ pada pilihan dan klik butang ***Start***.

Nota:

Sekiranya anda memilih *Automatically fix file system errors* untuk semak *partition* yang mengandungi Sistem Pengoperasian Windows, anda akan diminta untuk menjadualkan semula semakan pada masa anda akan *start* komputer akan datang.

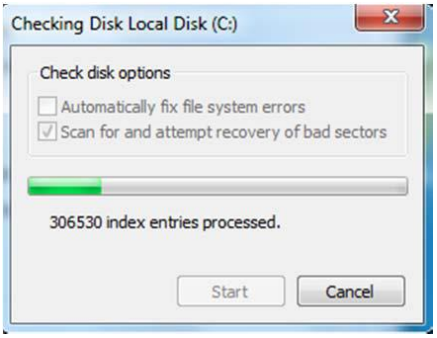
Klik butang ***Schedule disk check***.



Proses *error checking* ini akan dilaksanakan apabila anda *restart* komputer. Prosestersebut akan mengambil masa di antara 15 minit hingga 1 jam bergantung padasaiz *partition*/*hard disk*.

Nota:

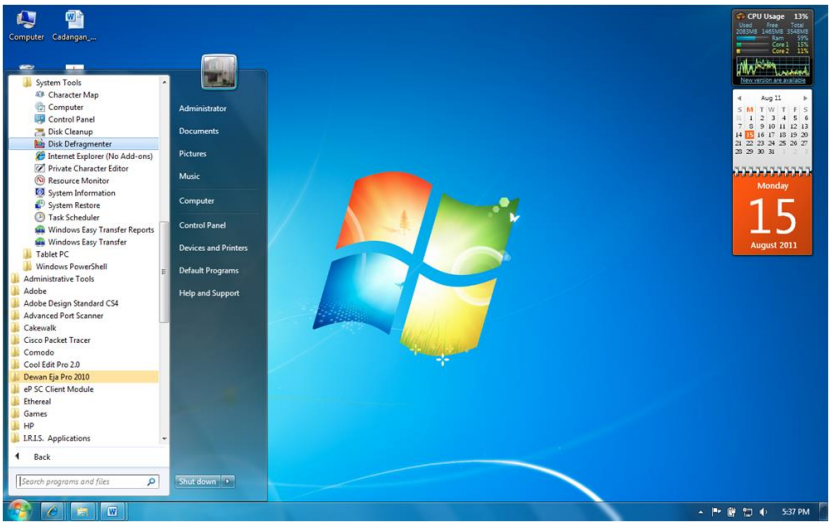
Sekiranya anda tidak memilih *Automatically fix file system errors*, proses error checking akan terus dijalankan dan skrin berikut akan dipaparkan. Tunggu sehingga proses selesai.



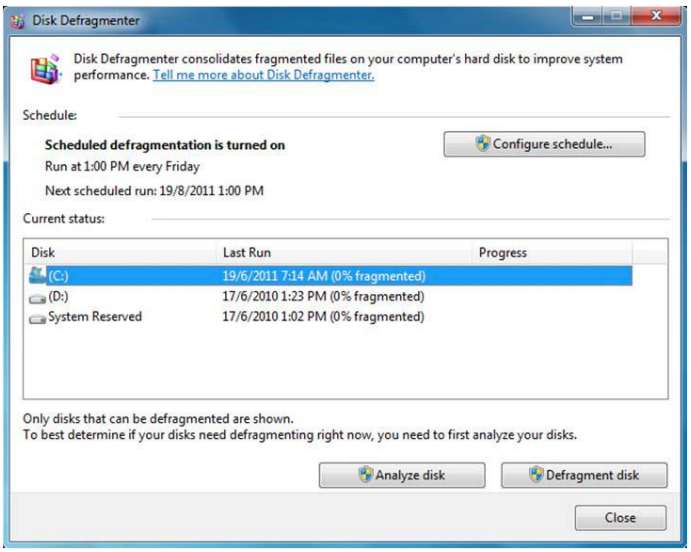
v) Proses tamat.

4. *Disk Defragmenter*

i) Klik ikon pada  *desktop* >***All programs*** >***Accessories*** >***System Tools*** >***Disk Defragmenter***.

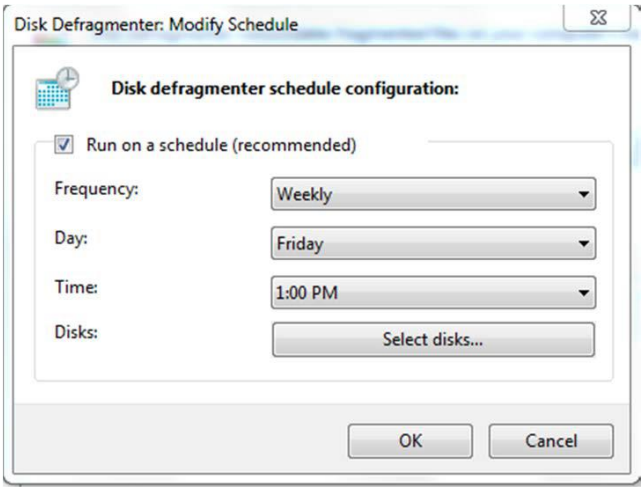


ii) Apabila skrin di bawah dipaparkan, anda diberi pilihan sama ada menjadualkan *defragmentation* atau laksanakan pada masa tersebut.



Pelaksanaan Defragmentation secara berjadual

Untuk pelaksanaan *Defragmentation* secara berjadual, pada skrin *Disk Defragmenter*, klik butang ***Configure schedule*** dan skrin berikut akan dipaparkan.

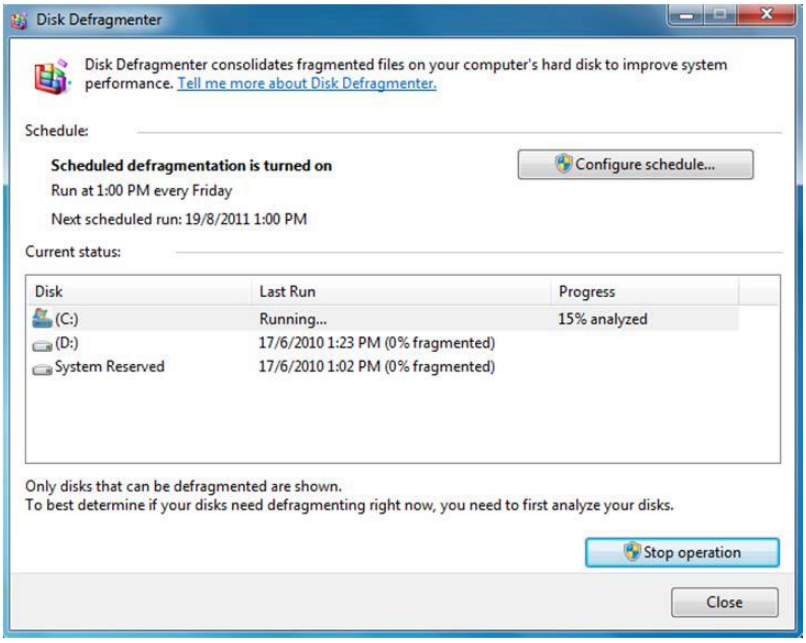


Lengkapkan butiran berikut dan klik butang ***OK***. Pelaksanaan *Disk Defragment* nanti akan dilaksanakan seperti yang telah dijadualkan.

Nota:

Pastikan komputer *On* pada masa *Disk Defragment* dijadualkan.

iii) Untuk melaksanakan *Disk Defragment* pada masa tersebut, pada skrin Disk Defragmenter, pilih disk yang hendak dilakukan *Disk Defragment* (sebagai contoh:
(C:) dan klik butang ***Defragment disk***.



iv) Tunggu sehingga proses selesai dan proses boleh dipantau pada ruangan *progress*.
(Contoh: progress 100%)

v) Proses tamat.

Lampiran VI

SEKSYEN TEKNOLOGI MAKLUMAT
BAHAGIAN KHIDMAT PENGURUSAN
JABATAN PERANCANGAN BANDAR DAN DESA SEMENANJUNG MALAYSIA

BORANG KEBENARAN PINJAMAN / MEMBAWA KELUAR PERALATAN ICT

NAMA : _____

BAHAGIAN/SEKSYEN : _____

TELEFON : _____

PERALATAN :

Bil	Jenis Peralatan	No Siri
1		
2		
3		
4		
5		

Tarikh Pinjaman : _____ hingga _____

Tujuan : _____

_____

Lokasi Penggunaan : _____

Adalah dimaklumkan bahawa saya akan bertanggungjawab sepenuhnya ke atas peralatan yang tersebut diatas yang dipinjam daripada Seksyen Teknologi Maklumat bermula dari tarikh peralatan tersebut diambil sehingga peralatan tersebut dipulangkan.

Akuan Penerimaan	Akuan Pemulangan
_____ (Tandatangan)	_____ (Tandatangan)
Nama : _____	Nama : _____
Tarikh : _____	Tarikh : _____

UNTUK KEGUNAAN SEKSYEN TEKNOLOGI MAKLUMAT

Diluluskan Oleh

Nama : ..... Tarikh : .....

Jawatan : .....

b.p. Ketua Seksyen Teknologi Maklumat
Bahagian Khidmat Pengurusan
Jabatan Perancangan Bandar Dan Desa Semenanjung Malaysia

Lampiran VII

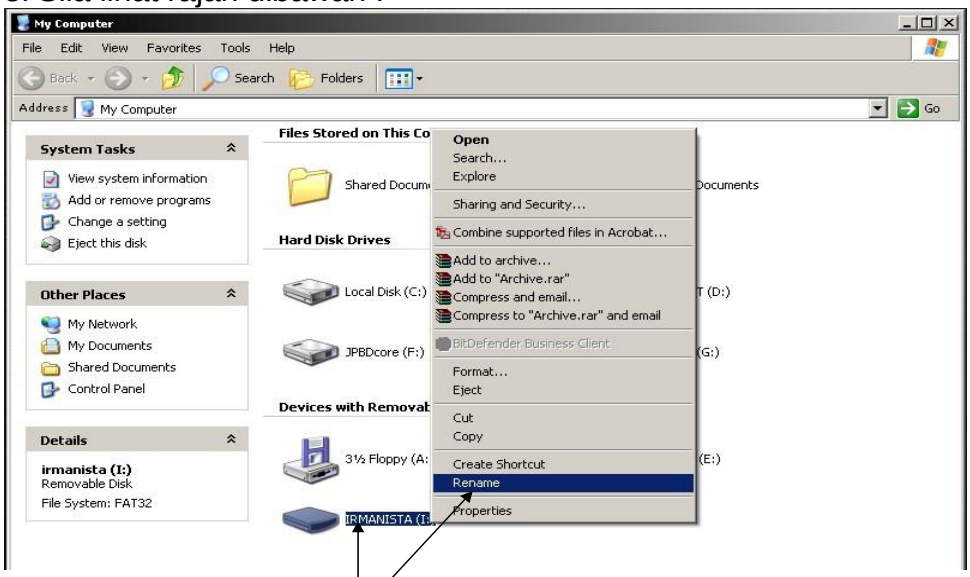
Tatacara Penggunaan Pendrive

Menamakan Pendrive / Thumbdrive Anda

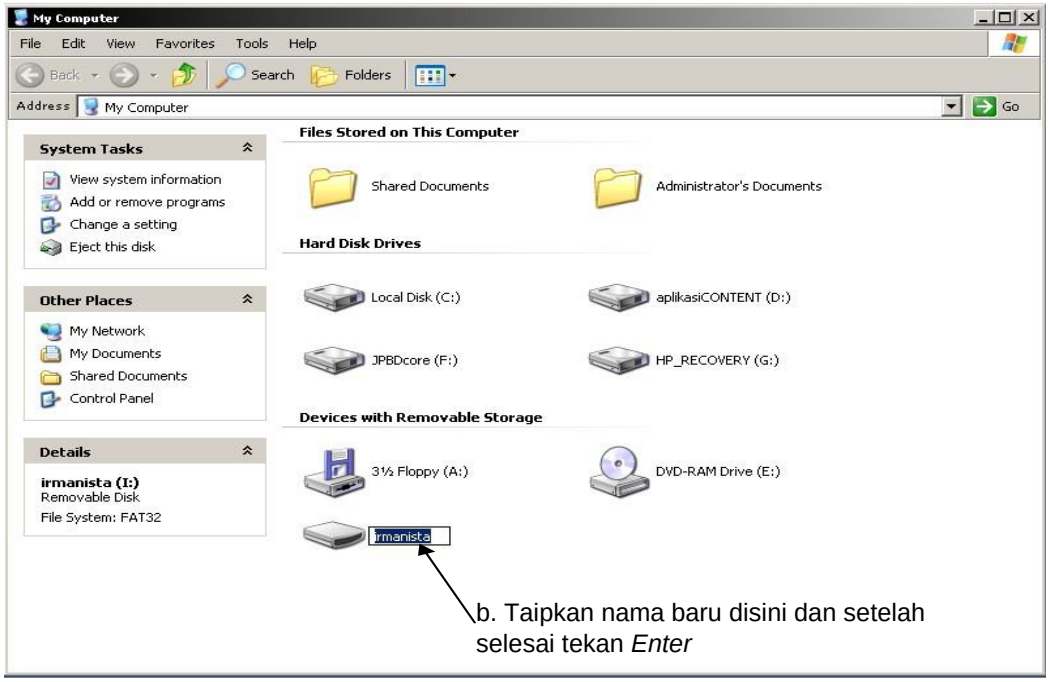
Langkah-langkah adalah seperti berikut :-

A : Cara Pertama

1. Masukkan pendrive / thumbdrive ke USB Port
2. Di desktop, double klik pada My Computer
3. Sila lihat rajah dibawah :-



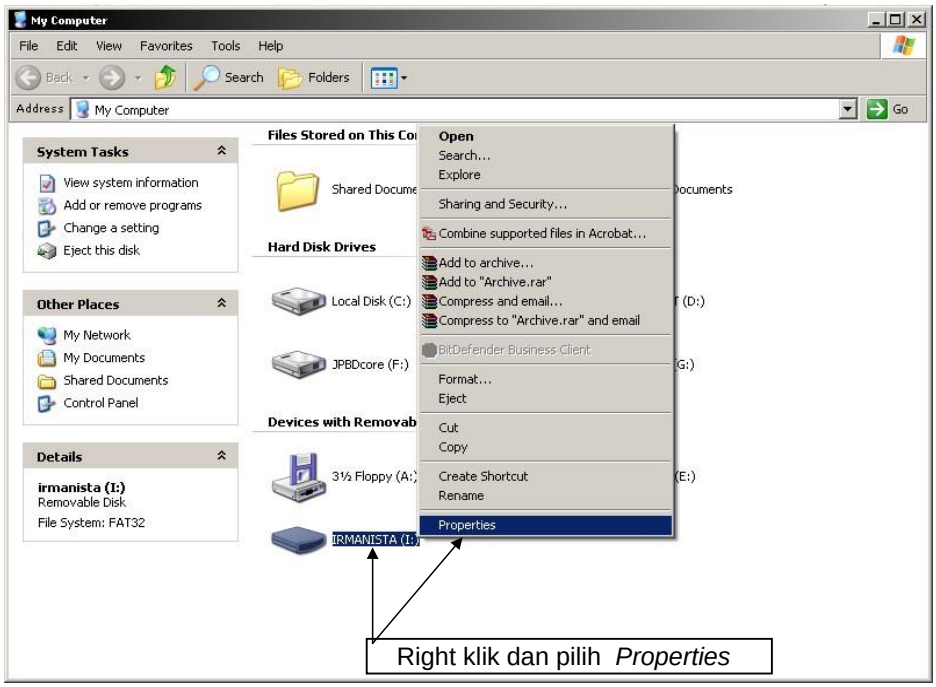
a. Right klik dan pilih Rename

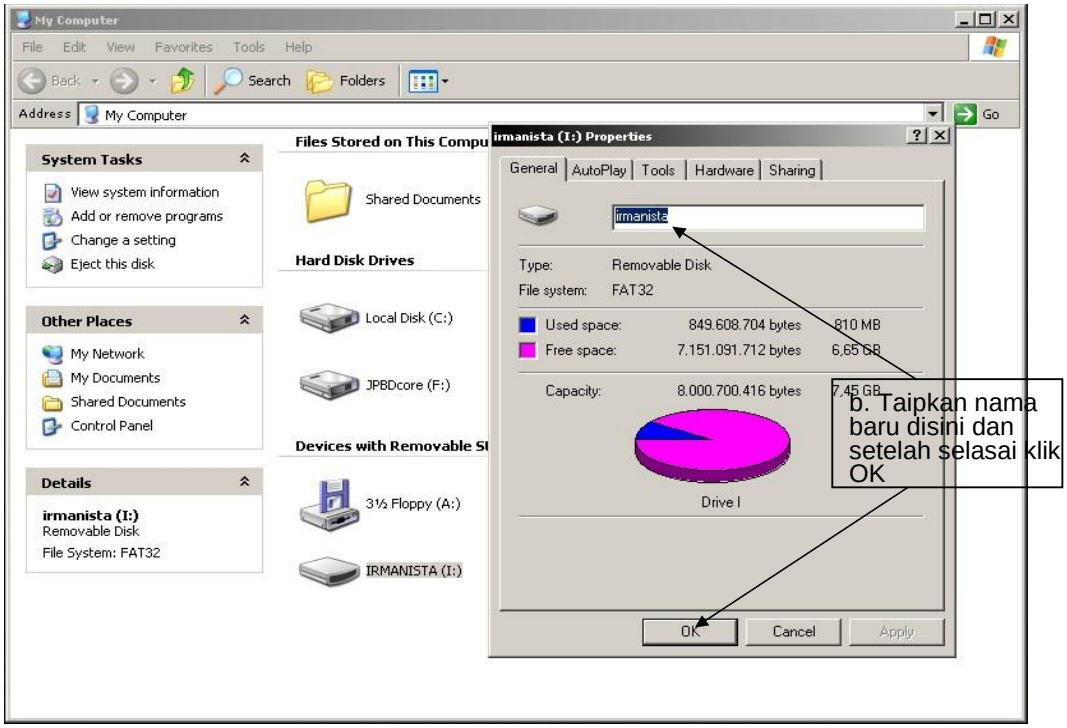


b. Taipkan nama baru disini dan setelah selesai tekan *Enter*

B : Cara Kedua

1. Sila lihat rajah dibawah :-





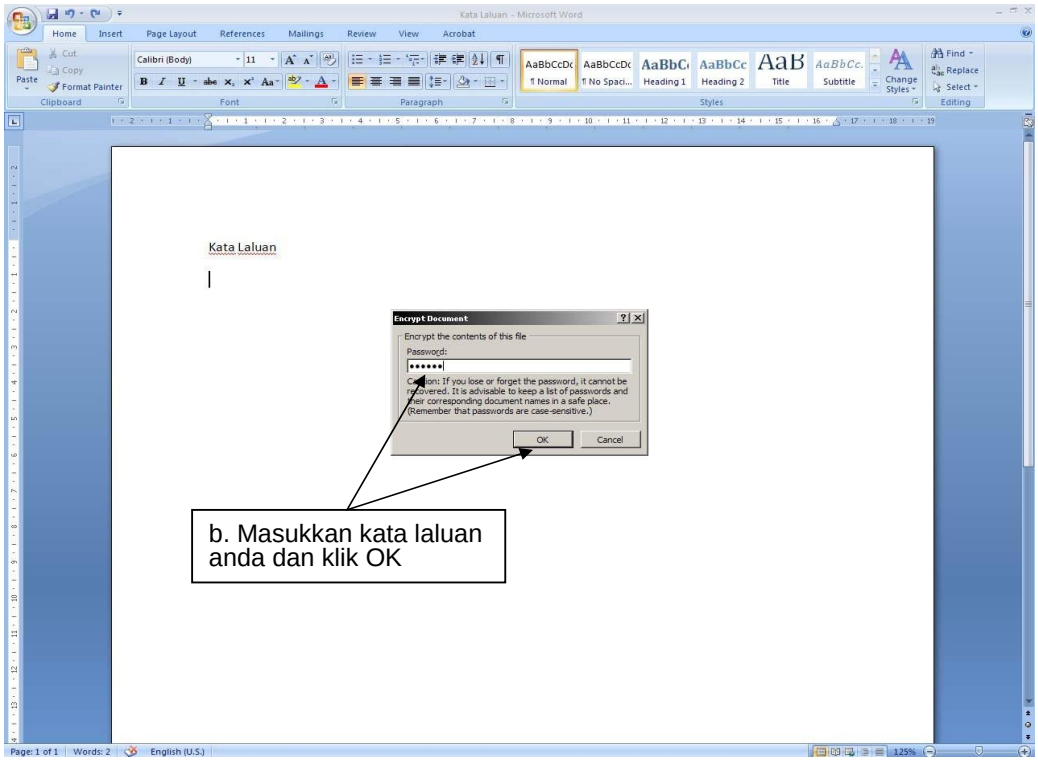
Lampiran VIII

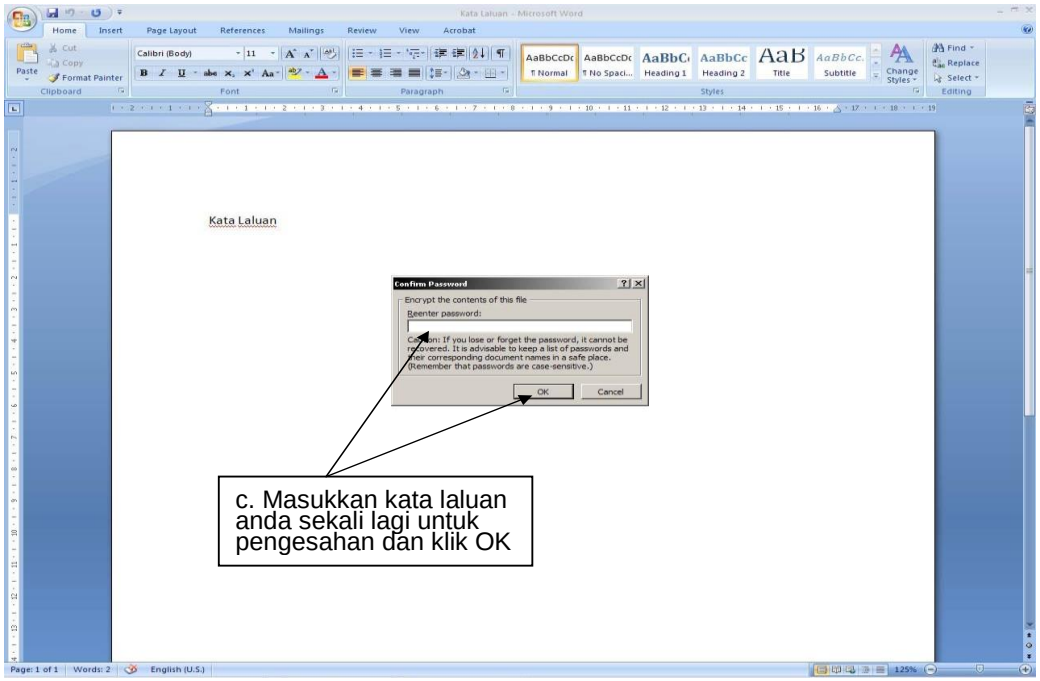
Tatacara Memberi Kata Laluan Pada Microsoft Word / OpenOffice Writer dan PDF File

Langkah-langkah adalah seperti berikut :-

A : Microsoft Word 2007

1. Buka Microsoft Word / Document Word anda dan ikuti langkah-langkah dibawah:-



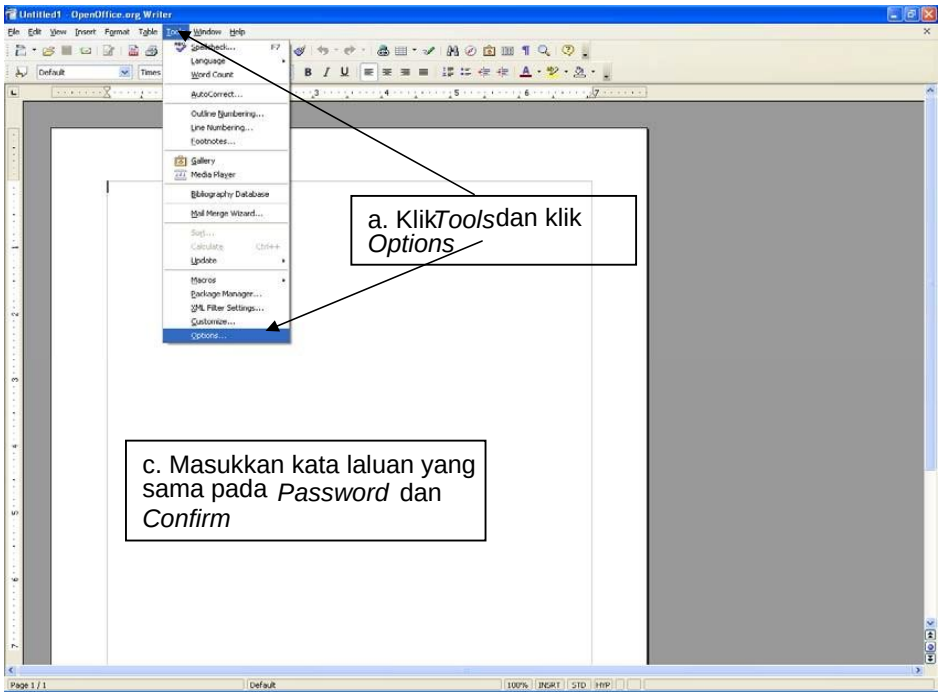


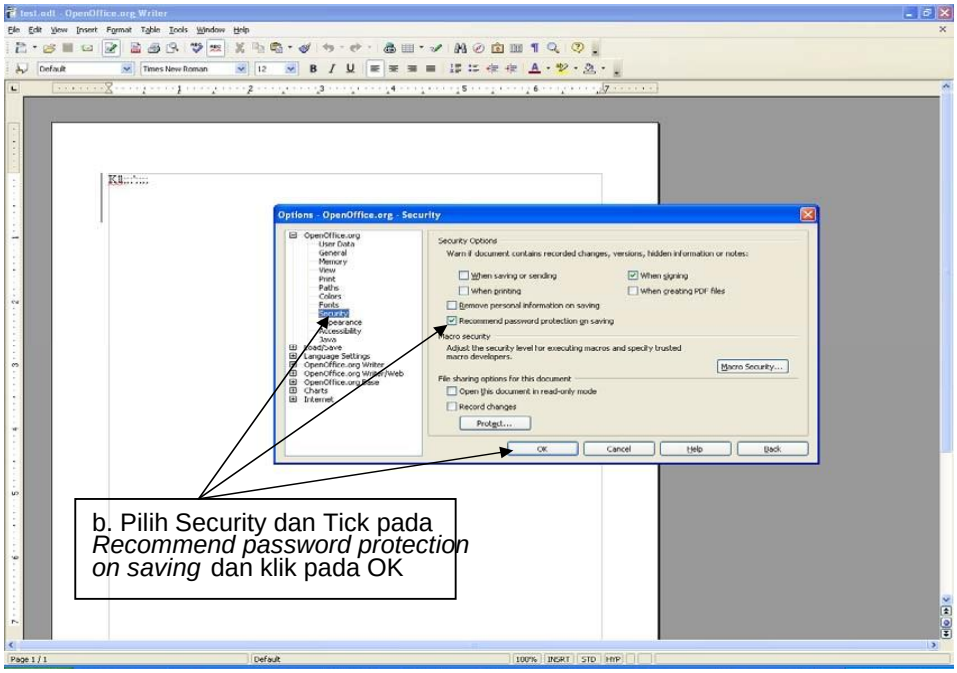
2. Setelah selasai, buka document word anda, dan masukkan kata laluan yang anda telah tetapkan.

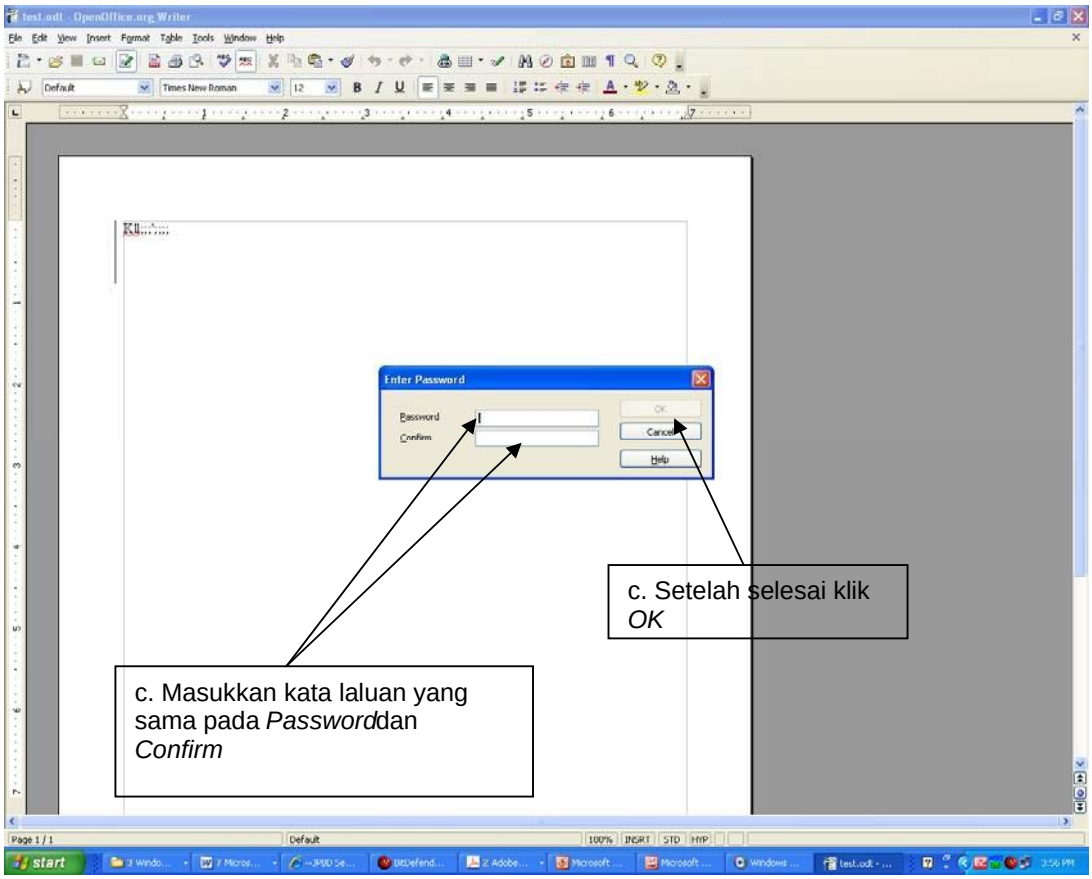
Perhatian : Sila ingat kata laluan anda, sebarang kata laluan yang telah ditetapkan tidak boleh direset kembali

B : OpenOffice Writer

1. Buka PDF File anda dan ikuti langkah-langkah dibawah :-





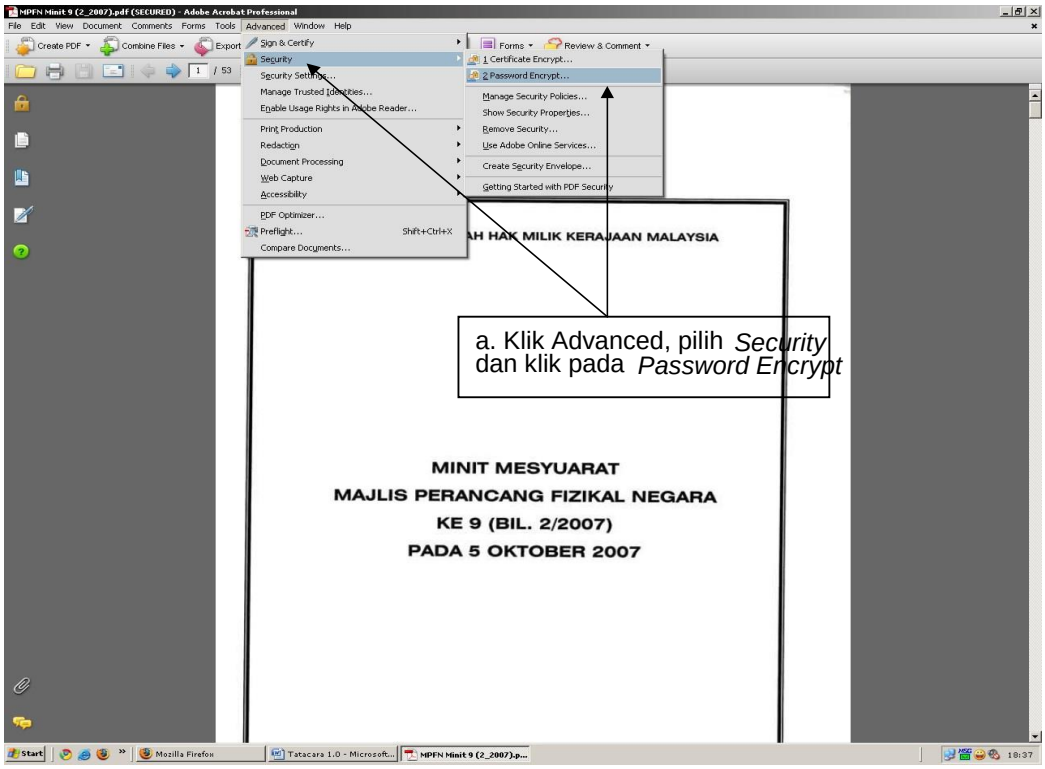


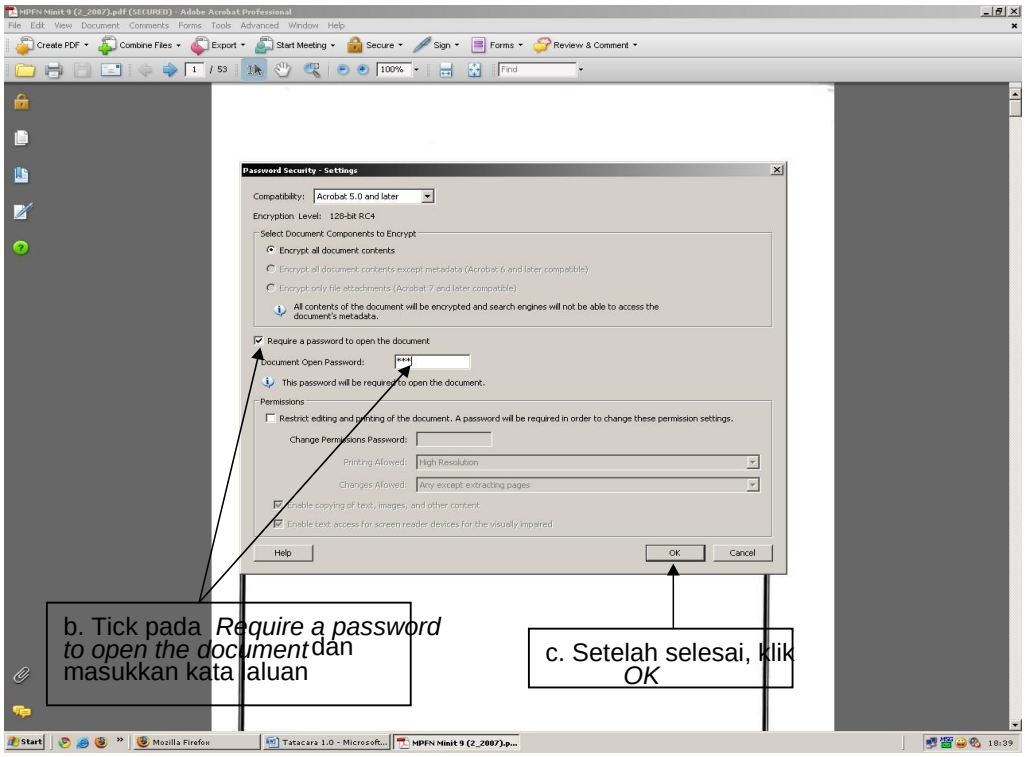
Setelah selasai, buka OpenOffice Writter anda, dan masukkan kata laluan yang anda telah tetapkan.

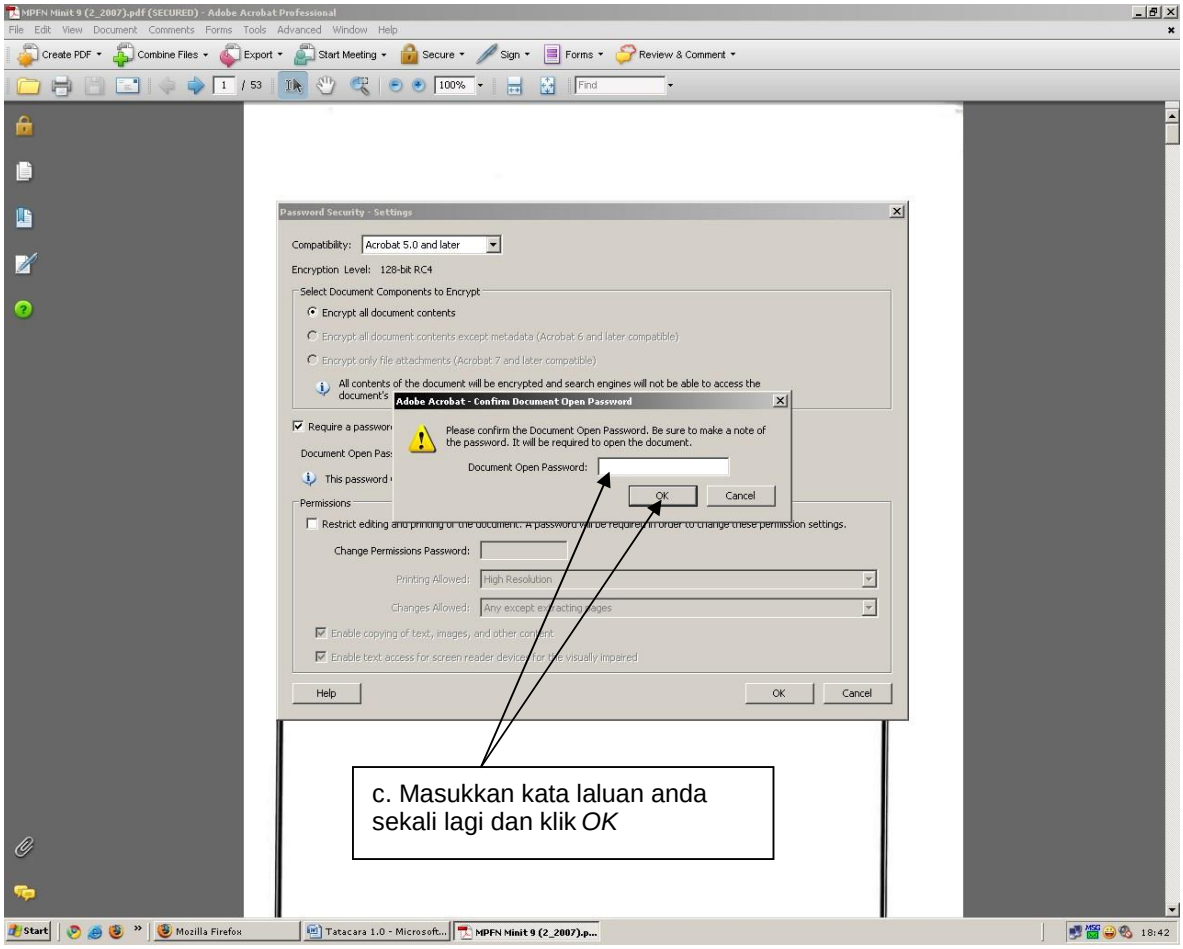
Perhatian : Sila ingat kata laluan anda, sebarang kata laluan yang telah ditetapkan tidak boleh direset kembali

C : PDF File

1. Buka PDF File anda dan ikuti langkah-langkah dibawah :-







2. Setelah selasai, buka PDF File anda, dan masukkan kata laluan yang anda telah tetapkan.

Perhatian : Sila ingat kata laluan anda, sebarang kata laluan yang telah ditetapkan tidak boleh direset kembali

Lampiran IX

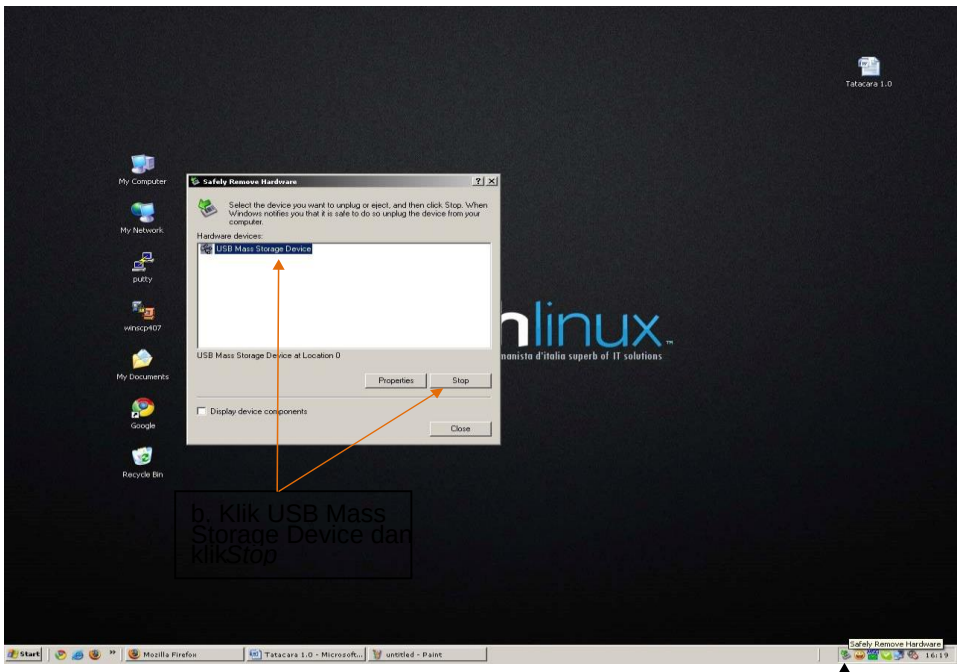
Tatacara Penggunaan Pendrive

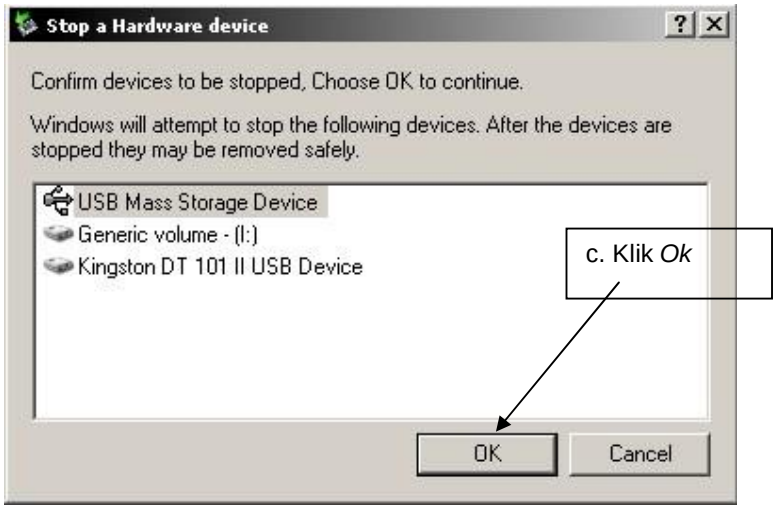
Mengeluarkan Pendrive / Thumbdrive dari USB Port

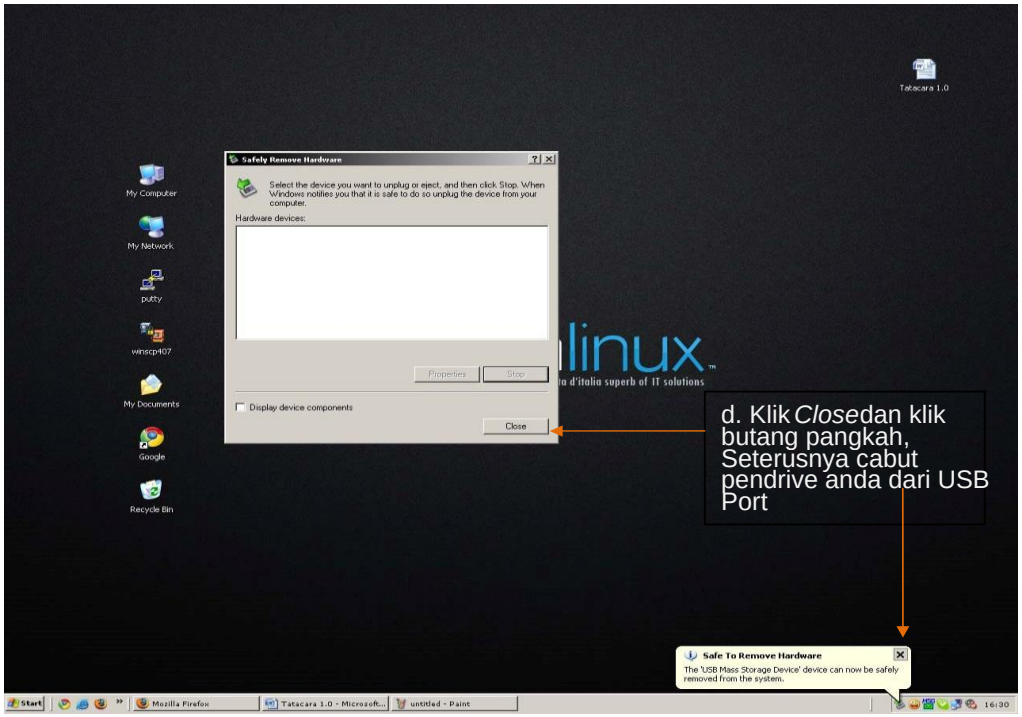
Langkah-langkah adalah seperti berikut :-

A : Cara Pertama

1. Tutup tetingkap pendrive anda untuk mengeluarkan device berkenaan dari PC
2. Sila lihat rajah dibawah :-

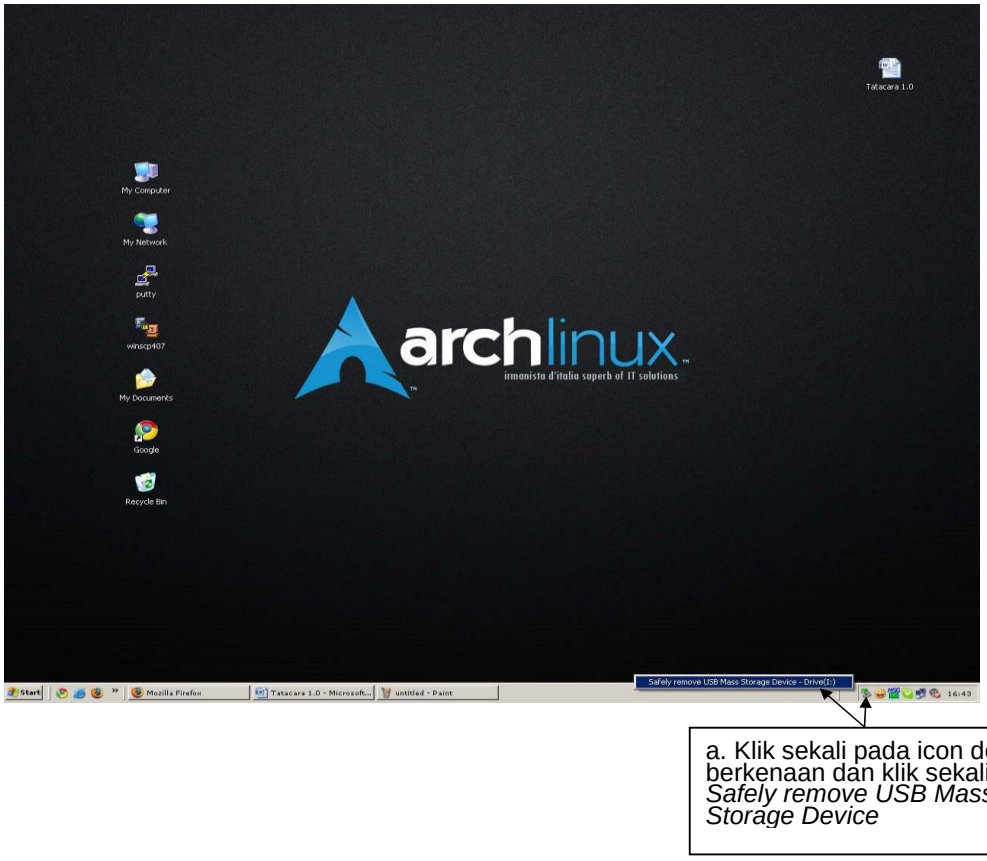


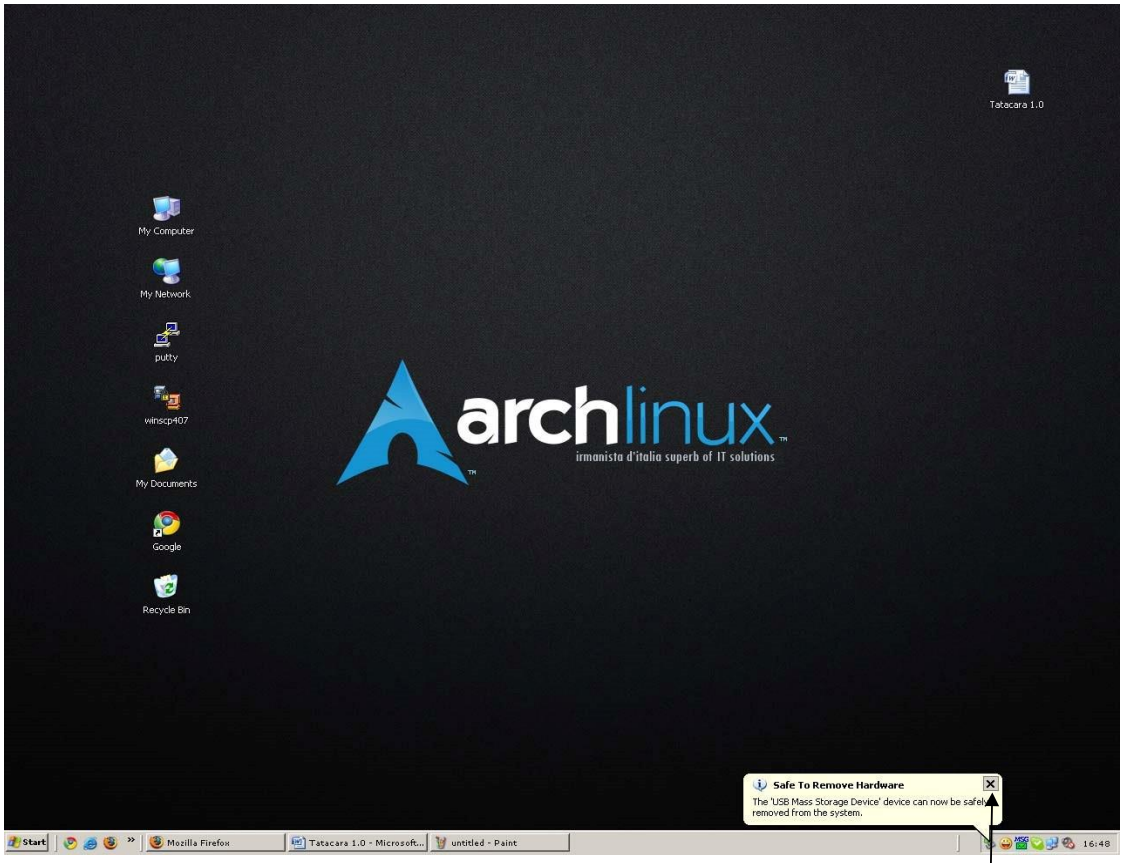




B : Cara Kedua

1. Sila lihat rajah dibawah :-





b. Klik butang pangkah, dan cabut pendrive anda dari USB Port

Glossary

(yang digunakan dalam GPKTMDK(ICT))

Worm (write once, read many) is a self-replicating virus that does not alter files but resides in active memory and duplicates

Sniffer is a program that monitors and analyzes network traffic.

Peer-to-peer (P2P) network is a network in which each computer functions as a client or server for other computers.

Virus is a program or programming code that replicates by being copied or initiating its copying to.

Trojan horse is a program or utility that appears to be something useful or safe, but in reality is performing background tasks such as giving access to your computer or sending personal information to other computers

Trapdoor or manhole, a **backdoor** is a term used to describe a back way, hidden method, or other form of bypassing traditional security in order to gain access to a secure area.

Backup An operation or procedure that copies data to an alternative location, so it can be recovered if deleted or becomes corrupted.

Spyware is used to describe a software program that is intentionally installed on a computer by to monitor what other users of the same computer are doing.

Service Pack, a **SP** is a large update containing several fixes and updates for MicrosoftWindowsoperating systems

Disk **Cleanup** enables users to remove files that are no longer needed or that can be safely deleted.

ScanDisk is a Windows utility used to check your hard disk for errors and to correct problems that are found.

Defragmentation is a used to describe the process of reorganizing a hard drive's data to help increase the proficiency of accessing the data and prevent file fragmentation.

Compress is the process of taking one or more files and making them smaller by using a compression algorithm.