



PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

MICROSOFT OFFICE 2007

UNIT PEMODENAN TADBIRAN DAN PERANCANGAN

PENGURUSAN MALAYSIA (MAMPU)

JABATAN PERDANA MENTERI

1.0 OBJEKTIF

Prosedur ini bertujuan untuk memastikan perlindungan maklumat terperingkat dalam format elektronik dilaksanakan bagi melindungi data dan maklumat dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin serta menjamin kesinambungan perkhidmatan kerajaan.

2.0 SKOP

Prosedur ini diguna pakai untuk melindungi maklumat terperingkat MAMPU yang disedia, disimpan dan diedar secara elektronik dengan menggunakan kaedah enkripsi daripada ancaman persekitaran.

3.0 RUJUKAN

- (a) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 01 Oktober 2000, Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
- (b) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 15 Januari 2002, *Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) Version 2.0*; dan
- (c) Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 02 April 2009, Dasar Keselamatan ICT MAMPU versi 5.2.

4.0 DEFINISI

Bil	Istilah	Keterangan
4.1	Rahsia besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada MAMPU.
4.2	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan MAMPU, menyebabkan kerosakan besar kepada kepentingan dan martabat MAMPU atau memberi keuntungan besar kepada pihak luar.
4.3	Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan MAMPU tetapi memudaratkan kepentingan atau martabat MAMPU atau kegiatan Kerajaan atau orang perseorangan atau akan menjatuhkan imej MAMPU atau akan menguntungkan pihak luar.
4.4	Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.

5.0 KLASIFIKASI DAN PENGENDALIAN MAKLUMAT

5.1 Pengelasan Maklumat

Maklumat rasmi hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan sepertimana yang dinyatakan di dalam Arahan Keselamatan:

- i. Rahsia Besar;
- ii. Rahsia;
- iii. Sulit; atau
- iv. Terhad

5.2 Perlindungan Maklumat Elektronik

Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat elektronik, langkah-langkah berikut hendaklah dipatuhi:

- i. Memastikan penyimpanan dan pendedaran maklumat elektronik adalah selamat dan terjamin;
- ii. Menggunakan tanda atau label keselamatan seperti rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
- iii. Menggunakan enkripsi ke atas dokumen terperingkat yang disedia, disimpan dan diedar secara elektronik.

5.3 Perlindungan Maklumat Elektronik Melalui Kaedah Enkripsi

Perlindungan maklumat digital atau elektronik memerlukan kaedah pengendalian media yang berbeza seperti penggunaan enkripsi. Kaedah ini melibatkan aktiviti penukaran teks biasa (*plaintext*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses dekripsi digunakan.

Pengendalian Maklumat	Rahsia Besar	Rahsia	Sulit	Terhad	Terbuka
Penyimpanan					
Penyimpanan dalam Media Tetap / Media Boleh tukar (Fixed disk and exchangeable)	Enkripsi maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.			Tidak diperlukan	
Menghantar / Memindahkan					
Menghantar maklumat melalui Rangkaian Awam	Menggunakan kaedah enkripsi			Tidak diperlukan	

Jadual 1: Pengendalian Maklumat Elektronik

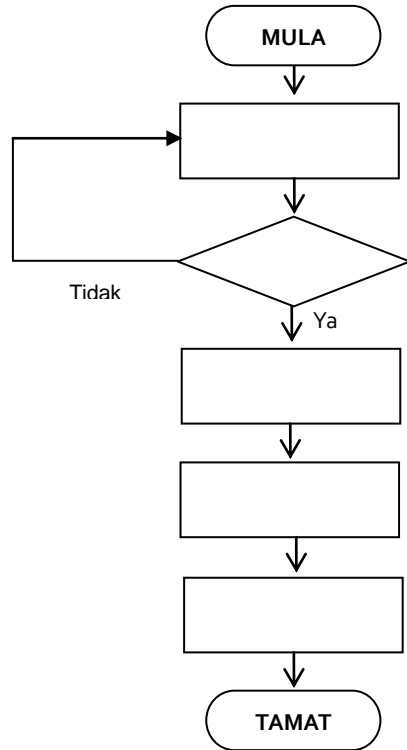
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

Enkripsi / Dekripsi

- i. Salah satu kaedah yang praktikal untuk memelihara data adalah dengan menukarkannya ke dalam bentuk rahsia di mana penerima yang sah sahaja dapat memahaminya.
- ii. Enkripsi (*Encryption*) ~ pengirim menukarkan mesej asal ke bentuk rahsia dan menghantar kepada penerima.
- iii. Dekripsi (*Decryption*) ~ menterbalikkan kembali proses enkripsi supaya mesej ditukar ke dalam bentuk yang asal.

Proses Enkripsi / Dekripsi

- i. Pengirim menggunakan algorithma enkripsi dan kunci untuk menukarkan data asal (*plaintext*) ke dalam bentuk data yang disulitkan (*cipher text*)
- ii. Penerima menggunakan algorithma dekripsi dan kunci untuk menukarkan *cipher text* kembali ke data asal (*plaintext*).
- iii. Kaedah enkripsi dan dekripsi boleh dibahagikan kepada 2 kategori:
 - *Conventional (secret key / symmetric)*
 - *Public key (asymmetric)*



Laksanakan pengelasan dan pelabelan maklumat rasmi mengikut pengelasannya seperti dalam Arahan Keselamatan

Telah dikelaskan?

Rekod pengelasan dan pelabelan maklumat rasmi

Simpan maklumat dengan menggunakan enkripsi maklumat atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain

Hantar maklumat dengan menggunakan enkripsi maklumat sekiranya menggunakan rangkaian awam



PROSEDUR ENKRIPSI/DEKRIPSI APLIKASI MICROSOFT OFFICE 2007

**WORD
POWERPOINT
EXCEL**

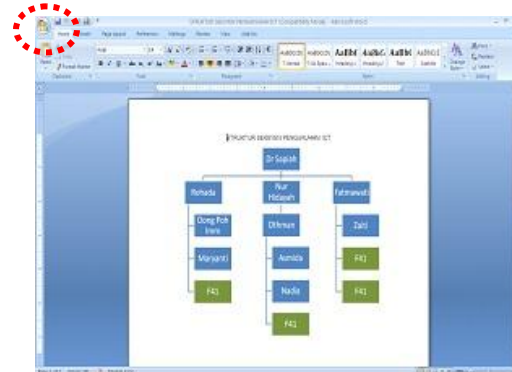
PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT WORD 2007

PENGENALAN

Aplikasi Microsoft Office sering digunakan dalam penghasilan dokumen seharian. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas.

LANGKAH-LANGKAH

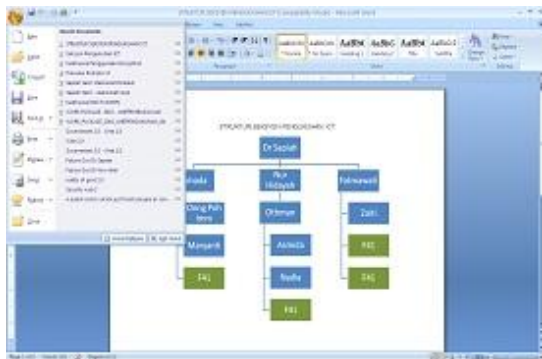
1. Sila klik '*Quick Access Toolbar*' (rujuk Rajah 1)



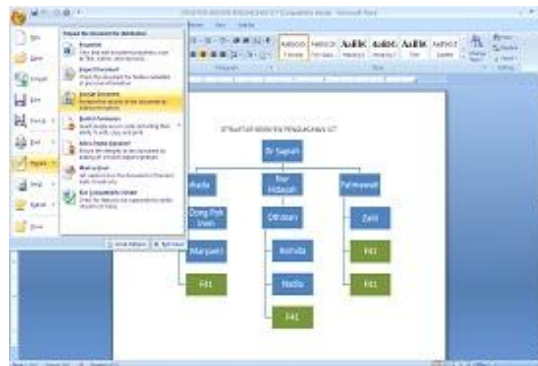
Rajah 1: Langkah 1

2. Sila pilih '**Prepare**' (rujuk Rajah 2).

3. Seterusnya klik '**Encrypt Document**' (rujuk Rajah 3).



Rajah 2: Menu Prepare



Rajah 3: Menu Encrypt Document

4. Sila masukkan kata laluan yang difikirkan sesuai (rujuk Rajah 4).

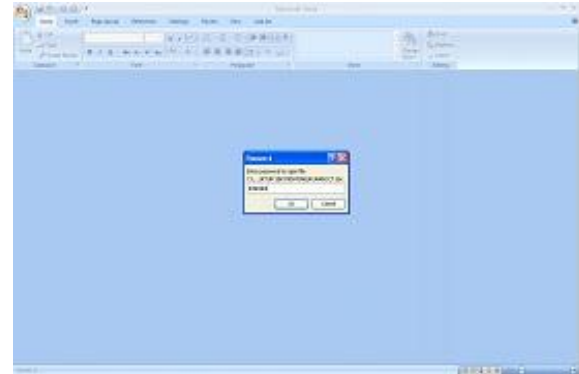
Nota:

Skrin pengesahan kata laluan akan dipaparkan setelah kata laluan dimasukkan buat kali pertama.

5. Sila Klik Ok setelah selesai.
6. Sila klik pilihan '**Save Document**' setelah selesai.

7. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen tersebut.

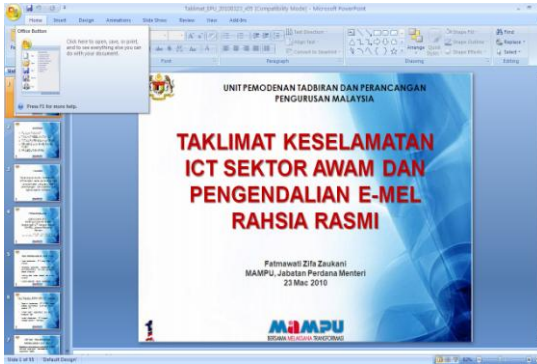
8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima (rujuk Rajah 5)



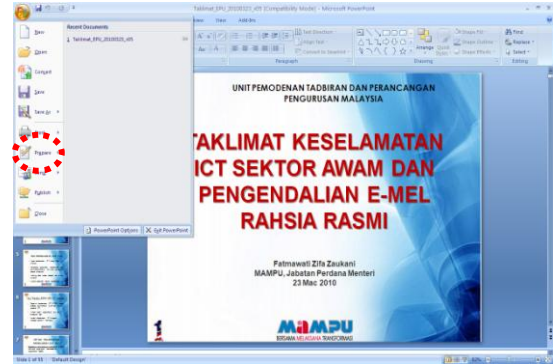
**PROSEDUR ENKRIPSI/DEKRIPSI
MICROSOFT POWERPOINT 2007**

LANGKAH-LANGKAH

1. Sila klik '*Quick Access Toolbar*' (rujuk Rajah 6).
2. Sila pilih '*Prepare*' (rujuk Rajah 7).



Rajah 6: Langkah 1



Rajah 7: Langkah 2

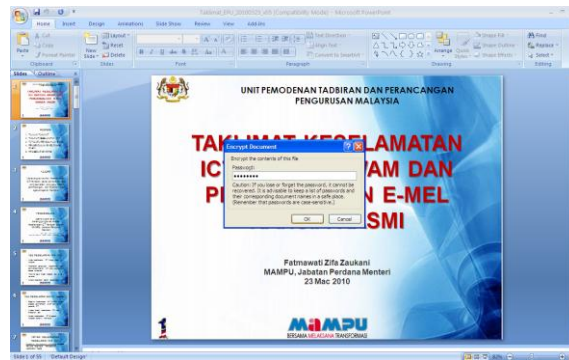
3. Seterusnya klik '**Encrypt Document**' (rujuk Rajah 8).
4. Sila masukkan kata laluan yang difikirkan sesuai (rujuk Rajah 9).

Nota:

- Skrin pengesahan kata laluan akan dipaparkan setelah kata laluan dimasukkan buat kali pertama.
5. Sila klik '**OK**' setelah selesai.

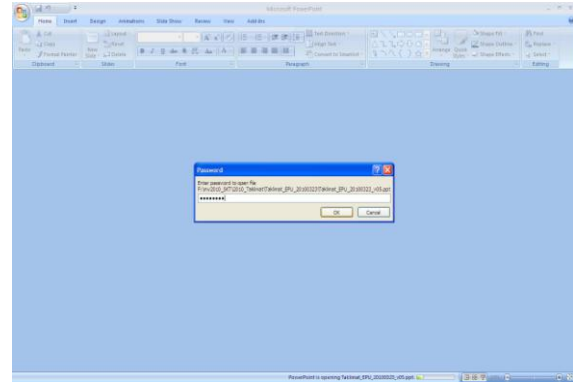


Rajah 8: Menu Encrypt Document



Rajah 9: Skrin Memasukkan Kata Laluan

6. Sila klik pilihan '**Save Document**' setelah selesai.
7. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.
8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima (rujuk Rajah 10).

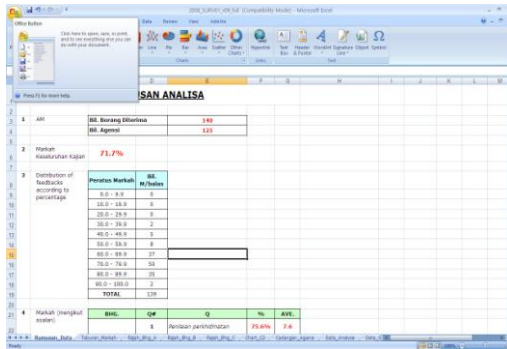


Rajah 10: Kata laluan untuk membuka dokumen

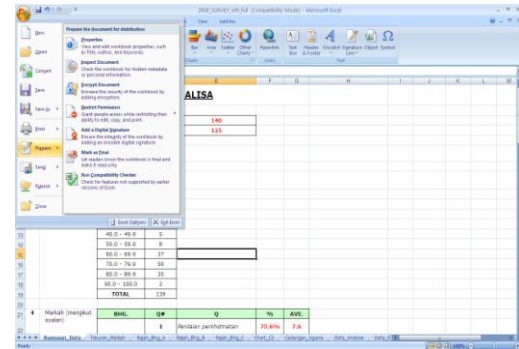
PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT EXCEL 2007

LANGKAH-LANGKAH

1. Sila klik '**Quick Access Toolbar**' (rujuk Rajah 11).
2. Sila pilih '**Prepare**' (rujuk Rajah 12).

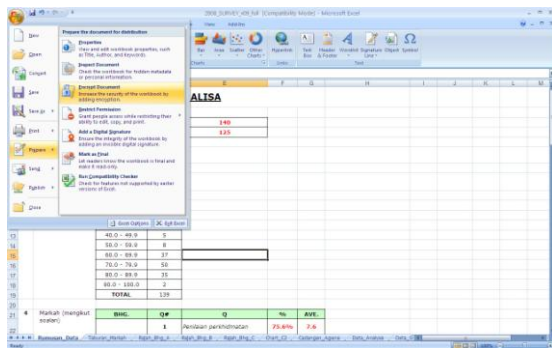


Rajah 11: Langkah 1



Rajah 12: Langkah 2

3. Seterusnya klik '**Encrypt Document**' (rujuk Rajah 13).

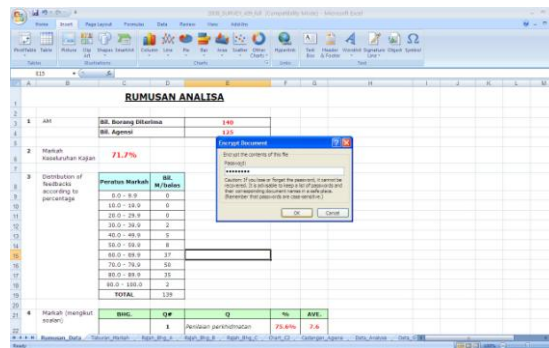


Rajah 13: Menu Encrypt Document

4. Sila masukkan kata laluan yang difikirkan sesuai (rujuk Rajah 14).

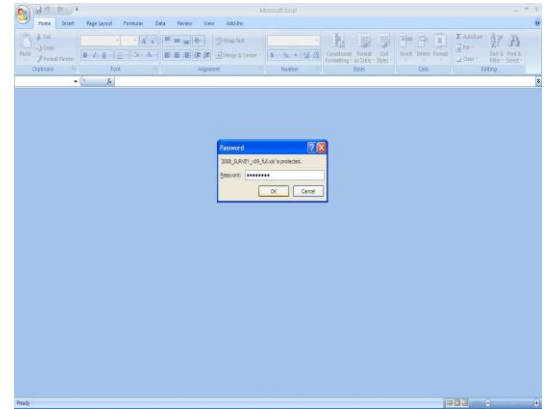
Nota:

Skrin pengesahan kata laluan akan dipaparkan setelah kata laluan dimasukkan buat kali pertama.



Rajah 14: Skrin Memasukkan Kata Laluan

5. Sila klik 'OK' setelah selesai.
6. Sila klik pilihan '**Save Document**' setelah selesai.
7. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.
8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima (rujuk Rajah 15).



Rajah 15: Kata Laluan untuk Membuka Dokumen

DISEDIAKAN OLEH:

BAHAGIAN PEMATUHAN ICT
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)
JABATAN PERDANA MENTERI
ARAS 6, BLOK B2
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

www.mampu.gov.my

Telefon : 03-8872 3000 / 8872 5000

Faks : 03-8888 3721