



PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

MICROSOFT OFFICE 2003

**JABATAN HAL EHWAL AGAMA TERENGGANU
(JHEAT)**

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 Jheat 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 Terengganu 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 Jheat .
4.2	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Jheat, menyebabkan kerosakan besar kepada kepentingan dan martabat Jheat 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 Jheat tetapi memudaratkan kepentingan atau martabat Jheat atau kegiatan Kerajaan atau orang perseorangan atau akan menjatuhkan imej Jheat 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
- iv. Terhad

5.2 Perlindungan Maklumat Elektronik

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

- i. Memastikan penyimpanan dan pengedaran 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 Elektroni

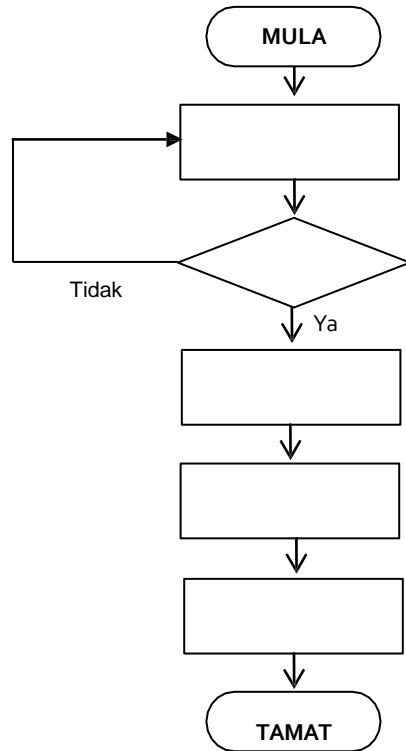
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

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 pengkelasan dan pelabelan maklumat rasmi mengikut pengelasan seperti dalam Arahan Keselamatan

Telah dikelaskan?

Rekod pengkelasan 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 2003

***WORD
POWERPOINT
EXCEL***



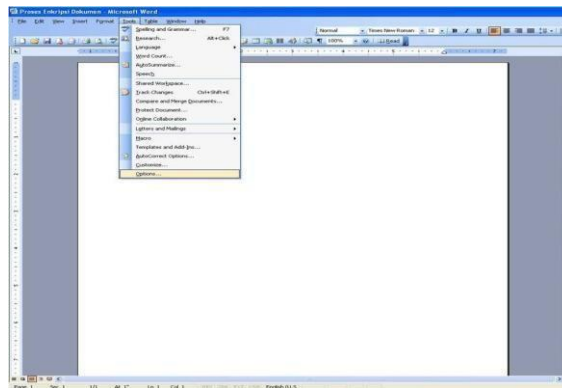
PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT WORD 2003

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 pada menu '**Tools**' dan daripada *pull-down menu* yang ditunjukkan, sila pilih '**Option**' (rujuk Rajah 1)

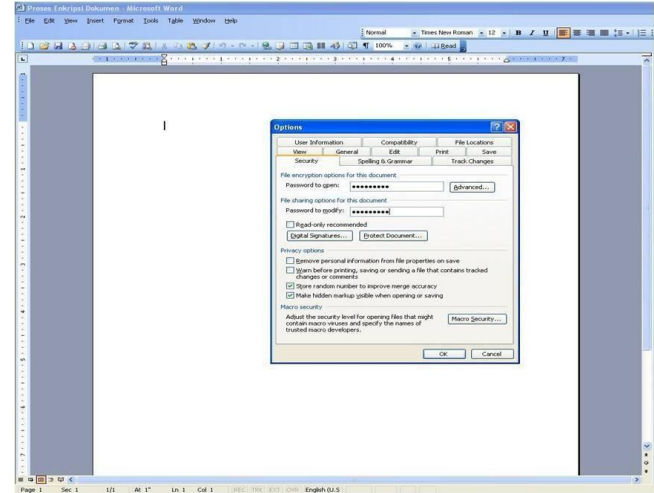


Rajah 1: Langkah 1

2. Skrin berikut akan dipaparkan (rujuk Rajah 2). Pilih tab '**Security**'
3. Masukkan kata laluan pada ruangan '**Password to open**'

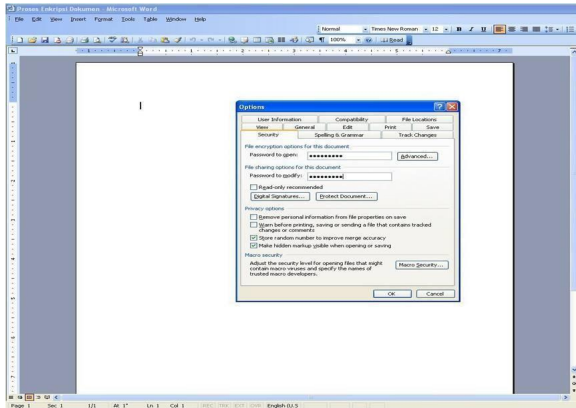
Nota: Jika pemunya dokumen berhasrat untuk tidak membenarkan penerima berkenaan mengubah isi kandungan dokumen, sila masukkan '**Password to modify**'

4. Klik '**OK**' setelah selesai



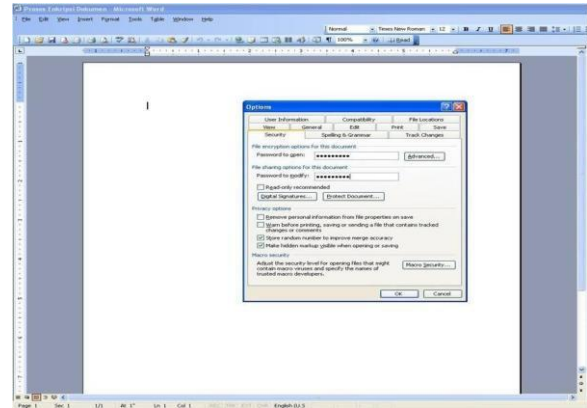
Rajah 2: Langkah 2 hingga 4

5. Skrin untuk memasukkan '**Password to Open**' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah 3).
6. Sila klik '**OK**'



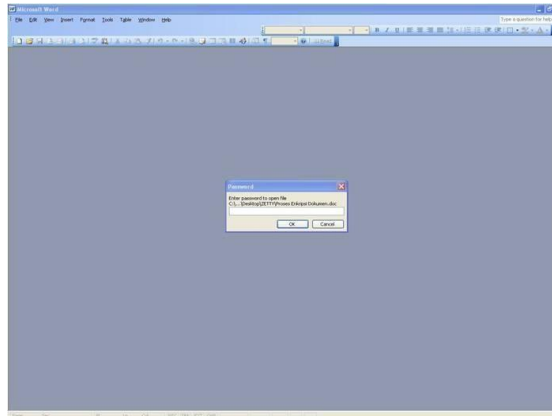
Rajah 3: Pengesahan Kata Laluan

7. Skrin untuk memasukkan '**Password to Modify**' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah 4).
8. Sila klik '**OK**'
9. Sila klik pilihan '**Save Document**' setelah selesai



Rajah 4: Pengesahan Kata Laluan untuk Membenarkan Dokumen Diubah

10. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.
11. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 5).

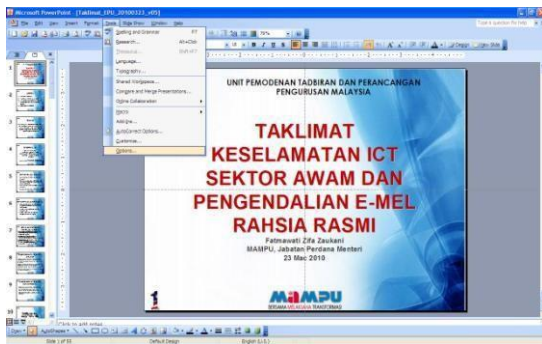


Rajah 5: Kata laluan untuk membuka dokumen

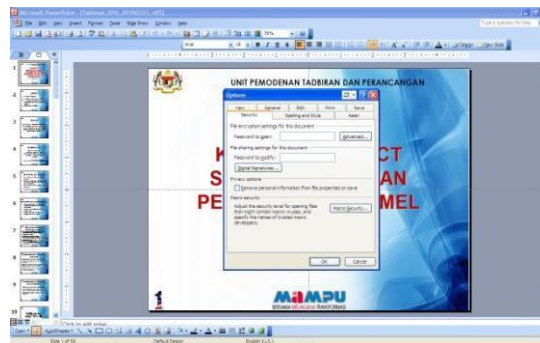


LANGKAH-LANGKAH

1. Sila klik pada menu **'Tools'** dan daripada *pull-down menu* yang ditunjukkan, sila pilih **'Option'** (rujuk Rajah 6).
2. Skrin berikut akan dipaparkan (rujuk Rajah 7).



Rajah 6: Langkah 1



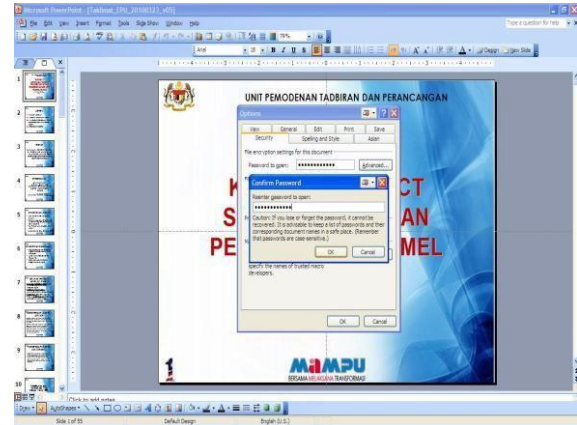
Rajah 7: Skrin 'Option'

- Pilih tab '**Security**'. Masukkan kata laluan pada ruangan '**Password to open**'.

Nota:

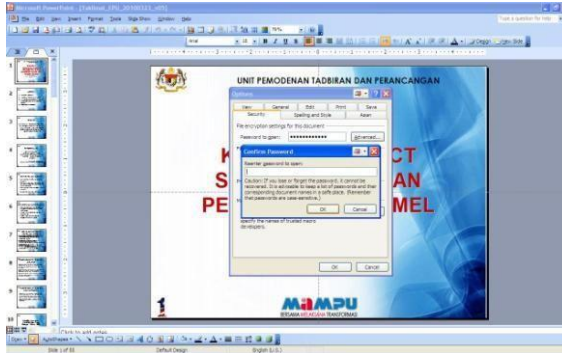
Jika pemunya dokumen berhasrat untuk tidak membenarkan penerima berkenaan mengubah isi kandungan dokumen, sila masukkan '**Password to modify**' (rujuk Rajah 8).

- Klik '**OK**' setelah selesai



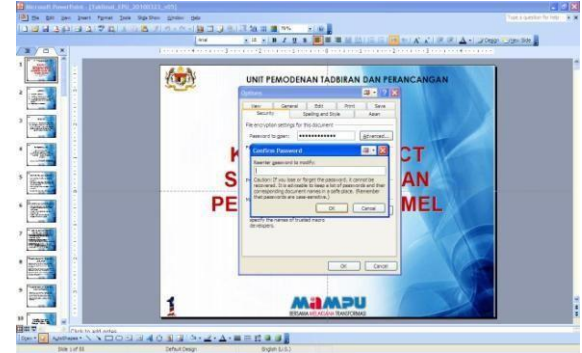
Rajah 8: Langkah 3 hingga 4

5. Skrin untuk memasukkan '**Password to Open**' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah9).
6. Sila klik '**OK**'.



Rajah 9: Pengesahan Kata Laluan

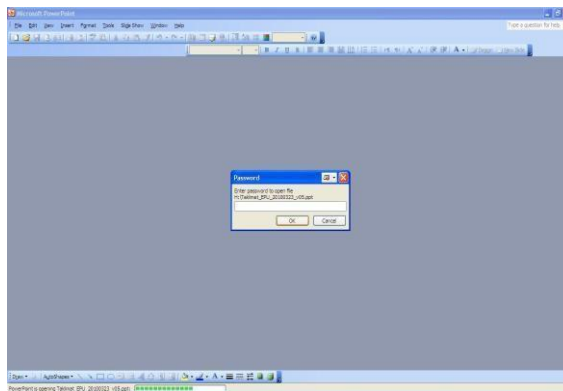
7. Skrin untuk memasukkan '**Password to Modify**' sebagai pengesahan kata laluan yang telah dipilih akan dipaparkan (rujuk Rajah10).
8. Sila klik '**OK**'.
9. Sila klik pilihan '**Save Document**' setelah selesai.



Rajah 10: Pengesahan Kata Laluan untuk Membenarka



10. Seterusnya pemunya dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.
11. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 11).



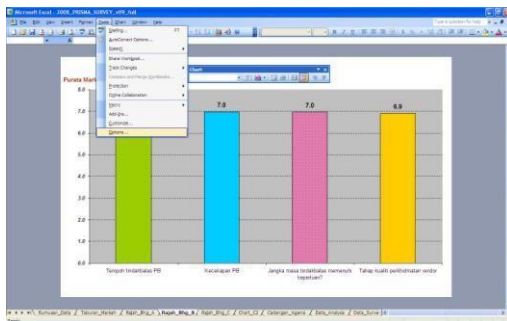
Rajah 11: Kata laluan untuk membuka dokumen



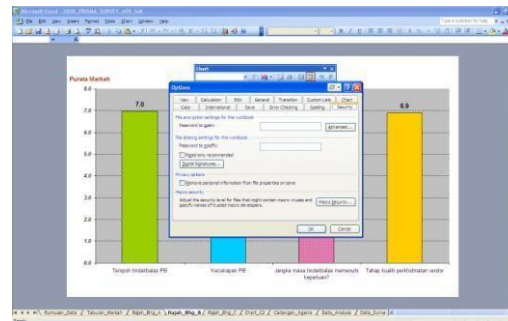
PROSEDUR ENKRIPSI/DEKRIPSI MICROSOFT EXCEL 2003

LANGKAH-LANGKAH

1. Sila klik pada menu '**Tools**' dan daripada *pull-down menu* yang ditunjukkan, sila pilih '**Option**' (rujuk Rajah 12).
2. Skrin berikut akan dipaparkan (rujuk Rajah 13)



Rajah 12: Langkah 1



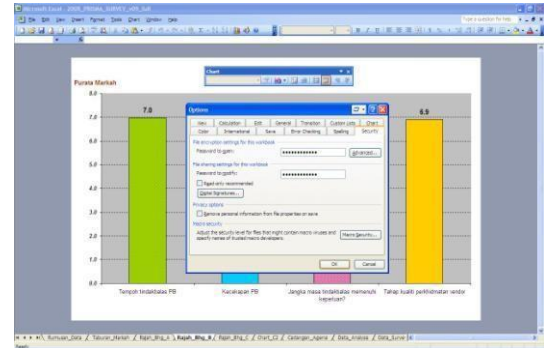
Rajah 13: Skrin 'Option'

3. Pilih tab '**Security**'. Masukkan kata laluan pada ruangan '**Password to open**'.

Nota:

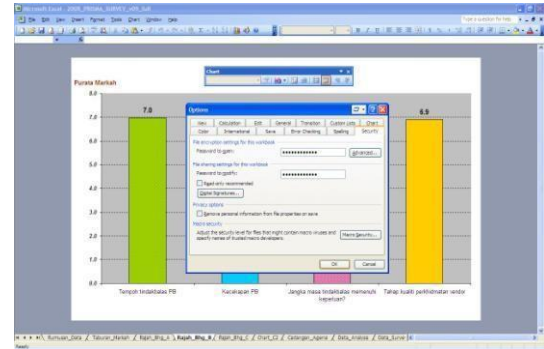
Jika pemunya dokumen berhasrat untuk tidak membenarkan penerima berkenaan mengubah isi kandungan dokumen, sila masukkan '**Password to modify**' (rujuk Rajah 14).

4. Klik '**OK**' setelah selesai. Skrin pengesahan kata laluan untuk membuka dokumen akan dipaparkan.



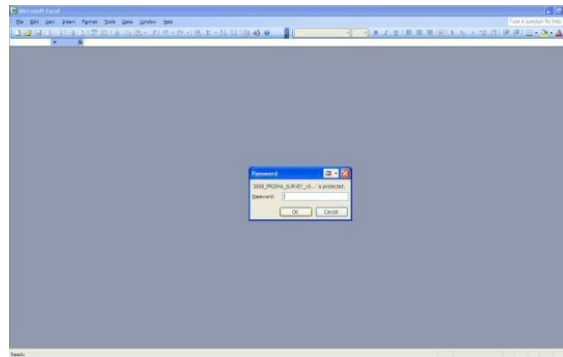
Rajah 14: Memajahtkan Kata Laluan

5. Sekiranya pemunya meletakkan kata laluan untuk mengubah dokumen, skrin untuk pengesahan kata laluan untuk mengubah dokumen akan dipaparkan (rujuk Rajah 16).
6. Sila klik pilihan '**Save Document**' setelah selesai.



Rajah 16: Pengesahan kata laluan untuk membenarkan dokumen diubah

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 pihak lain (rujuk Rajah16).



Rajah 17: Kata laluan untuk membuka dokumen



JABATAN HAL EHWAL AGAMA TERENGGANU

DISEDIAKANOLEH:

UNIT TEKNOLOGI
MAKLUMAT
JABATAN HAL EHWAL
AGAMA