



**UNIT PENGURUSAN TEKNOLOGI MAKLUMAT
PEJABAT SETIAUSAHA KERAJAAN NEGERI
SEMBILAN DARUL KHUSUS**

**PROSEDUR ENKRIPSI MAKLUMAT
TERPERINGKAT**

SUKNS-UPTM-ISMS-P2-014

ISO/IEC 27001:2013

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
 Nama : NURULLIZA BINTI HASSAN Jawatan : Penolong Pengarah Unit Pengurusan Teknologi Maklumat Pejabat Setiausaha Kerajaan N. Sembilan Tarikh : 10/4/2018	 Nama : AD ZAKI BIN ABDULLAH Jawatan : Penolong Pengarah Kanan Unit Pengurusan Teknologi Maklumat Pejabat Setiausaha Kerajaan N. Sembilan Tarikh : 24/5/2018	 Nama : ABD RAHIM BIN MOHD RAOF Jawatan : Pengarah, Unit Pengurusan Teknologi Maklumat Pejabat Setiausaha Kerajaan N. Sembilan Tarikh : 24/5/2018



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

KANDUNGAN

1.0	OBJEKTIF	1
2.0	SKOP	1
3.0	DEFINISI	1
4.0	RUJUKAN	2
5.0	KLASIFIKASI DAN PENGENDALIAN MAKLUMAT	2
6.0	PROSES ENKRIPSI MAKLUMAT TERPERINGKAT	3
7.0	LAMPIRAN	4
8.0	REKOD PINDAAN DOKUMEN	5
	LAMPIRAN A	
	LAMPIRAN B	
	LAMPIRAN C	



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

SINGKATAN

- a) P Pengarah
- b) PYB Pegawai Yang Bertanggungjawab



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

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 PSUKNS yang tersedia, disimpan dan diedar secara elektronik dengan menggunakan kaedah enkripsi daripada ancaman persekitaran.

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

Jadual 1: Pengelasan Dokumen Terperingkat



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

4.0 RUJUKAN

(a) Arahan Keselamatan

Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

(b) Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS) Version 2.0;

(c) Dasar Keselamatan ICT (DKICT) Negeri Sembilan versi terkini;

(d) Prosedur Pertukaran Maklumat SUKNS-UPTM-ISMS-P2-004; dan

(e) Prosedur Klasifikasi dan Pengendalian Maklumat SUKNS-UPTM-ISMS-P2-001

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 keboleh sediaan maklumat elektronik, langkah-langkah berikut hendaklah dipatuhi:

- i. Memastikan penyimpanan dan pengedaran maklumat elektronik adalah selamat dan terjamin;



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

- ii. Menggunakan tanda atau label keselamatan seperti i rahsia besar, rahsia, sulit atau terhad pada dokumen; dan
- iii. Menggunakan enkripsi ke atas dokumen terperingkat yang tersedia, 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 2: Pengendalian Maklumat Elektronik



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

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)

7.0 LAMPIRAN

- a) Lampiran A : Prosedur Enkripsi/Dekripsi Aplikasi Microsoft Word
- b) Lampiran B : Prosedur Enkripsi/Dekripsi Aplikasi Microsoft PowerPoint
- c) Lampiran C : Prosedur Enkripsi/Dekripsi Aplikasi Microsoft Excel



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

8.0 REKOD PINDAAN DOKUMEN

Tarikh	No.Keluaran/ Pindaan	Bab/Muka Surat	Keterangan Pindaan



SUKNS-UPTM-ISMS-P2-014

PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

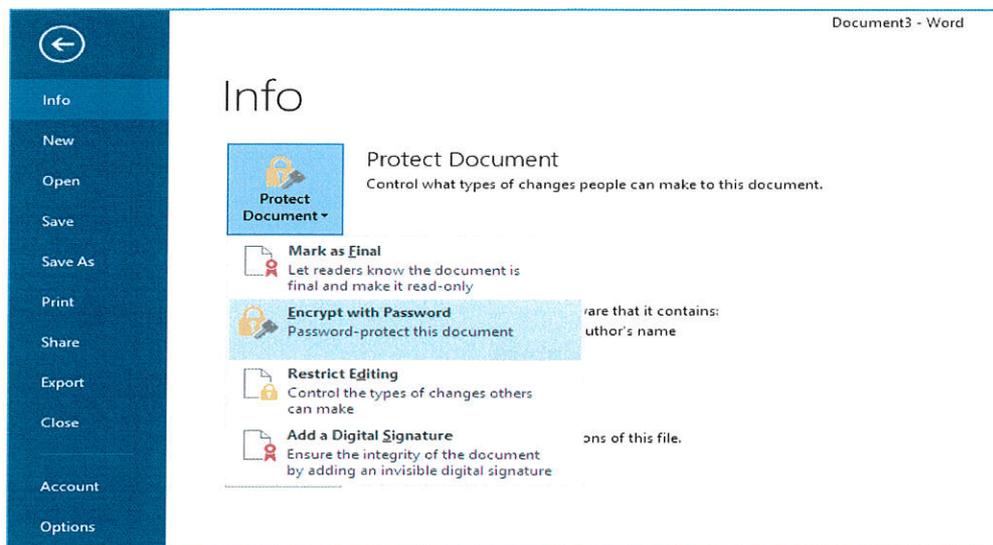
MANUAL ENKRIPSI/DEKRIPSI APLIKASI MICROSOFT WORD

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.

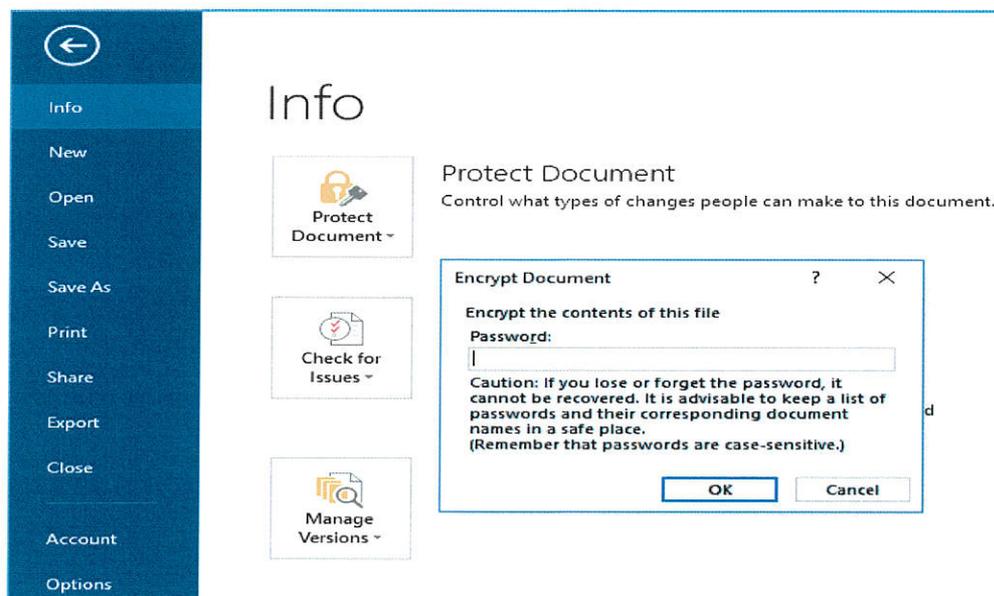
LANGKAH-LANGKAH

1. Sila klik pada menu 'FILE' dan daripada *pull-down menu* yang ditunjukkan, sila pilih 'Info' (rujuk Rajah 1). Klik 'Protect Document' dan pilih 'Encrypt with Password'.



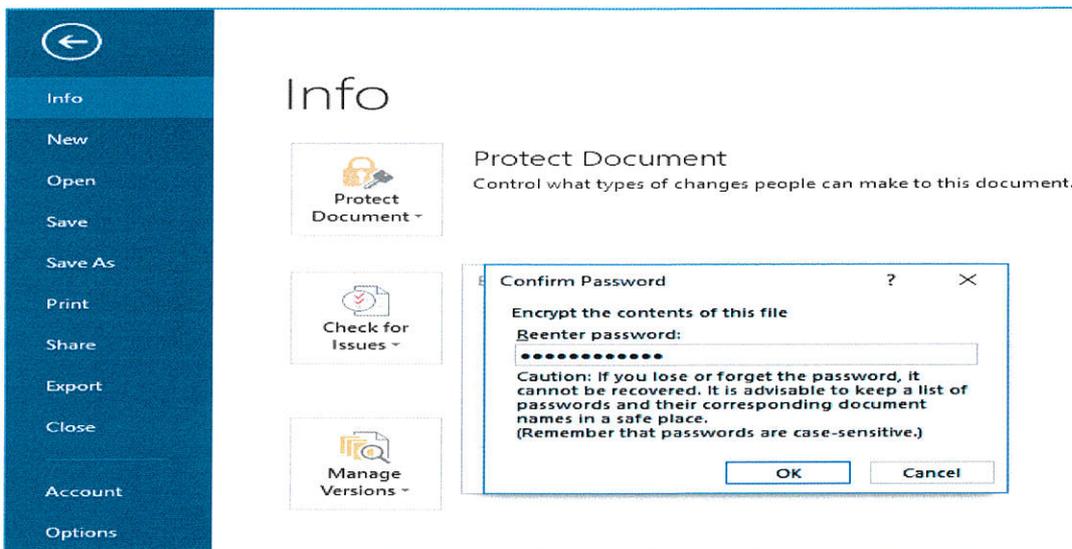
Rajah 1: Skrin perlindungan dokumen

2. Skrin berikut akan dipaparkan (rujuk Rajah 2).



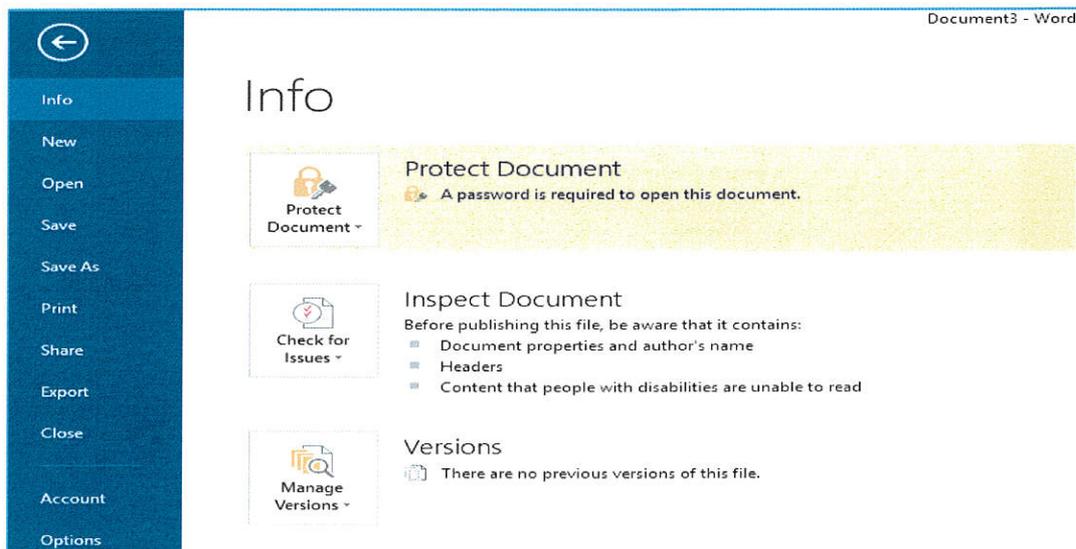
Rajah 2: Skrin paparan enkripsi dokumen

3. Masukkan kata laluan pada ruangan 'Password'. Klik 'OK' setelah selesai. Skrin 'Confirm Password' akan dipaparkan bagi pengesahan kata laluan. Masukkan kata laluan yang sama dan klik 'OK' (rujuk Rajah 3).

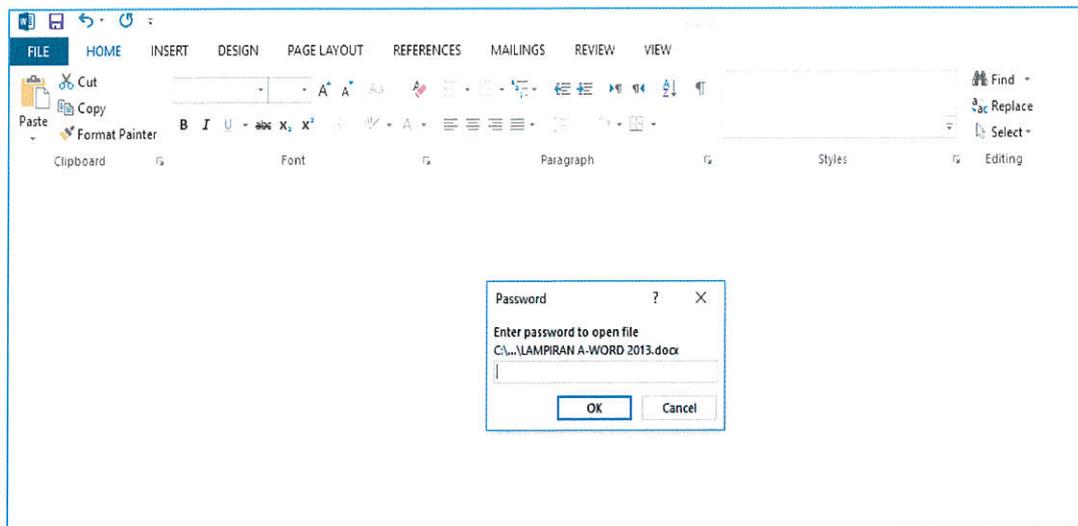


Rajah 3: Pengesahan kata laluan

4. Proses enkripsi anda selesai jika ruangan 'Protect Document' telah diwarnakan.



5. Seterusnya pemunya / penghantar dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.
6. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 4).



Rajah 4: Kata laluan untuk membuka dokumen

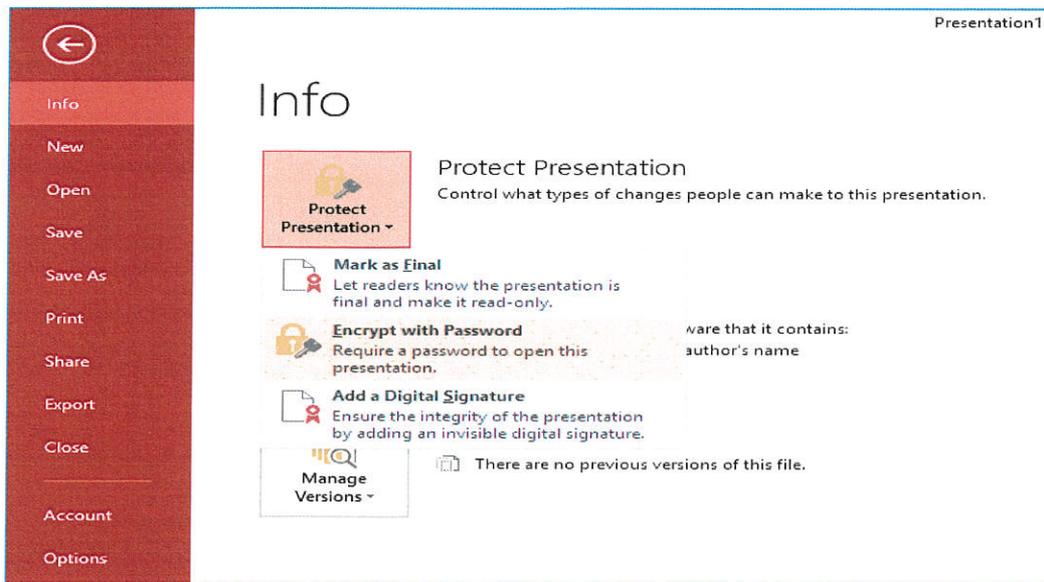
MANUAL ENKRIPSI/DEKRIPSI APLIKASI MICROSOFT POWERPOINT

PENGENALAN

Microsoft PowerPoint sering digunakan untuk membantu membangunkan format persembahan berdasarkan slaid. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas.

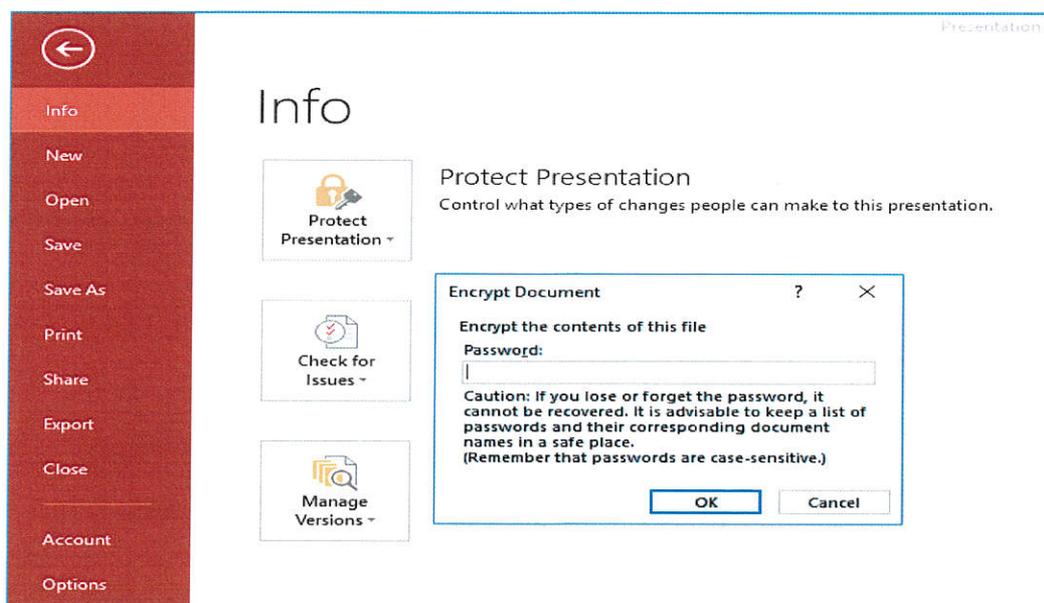
LANGKAH-LANGKAH

1. Sila klik pada menu 'FILE' dan daripada *pull-down menu* yang ditunjukkan, sila pilih 'Info' (rujuk Rajah 1). Klik 'Protect Presentation' dan pilih 'Encrypt with Password'.



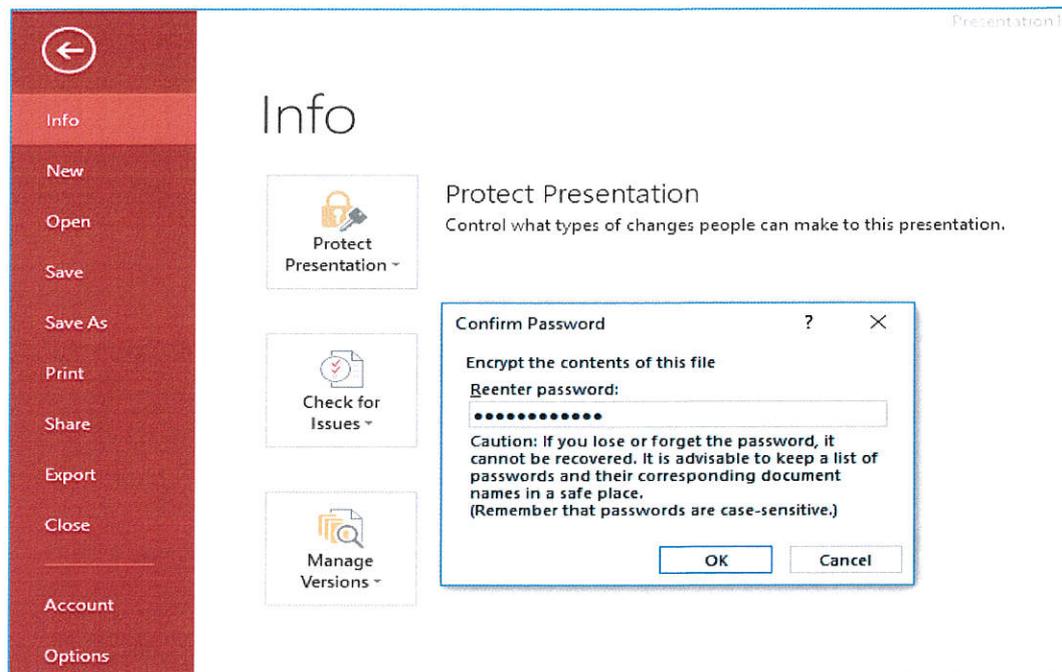
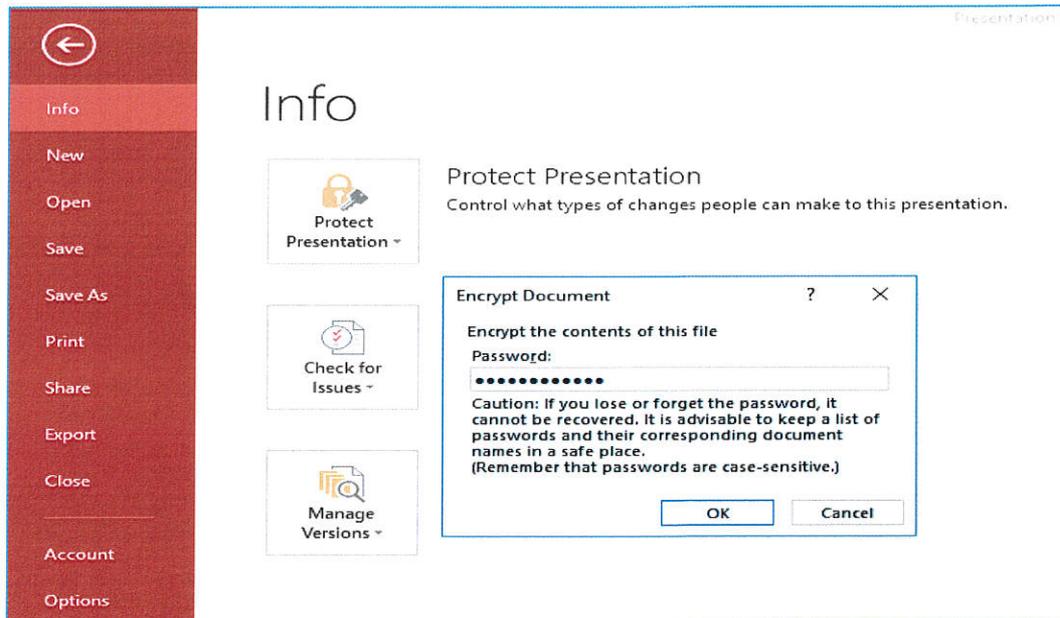
Rajah 1: Skrin perlindungan persembahan

2. Skrin berikut akan dipaparkan (rujuk Rajah 2).



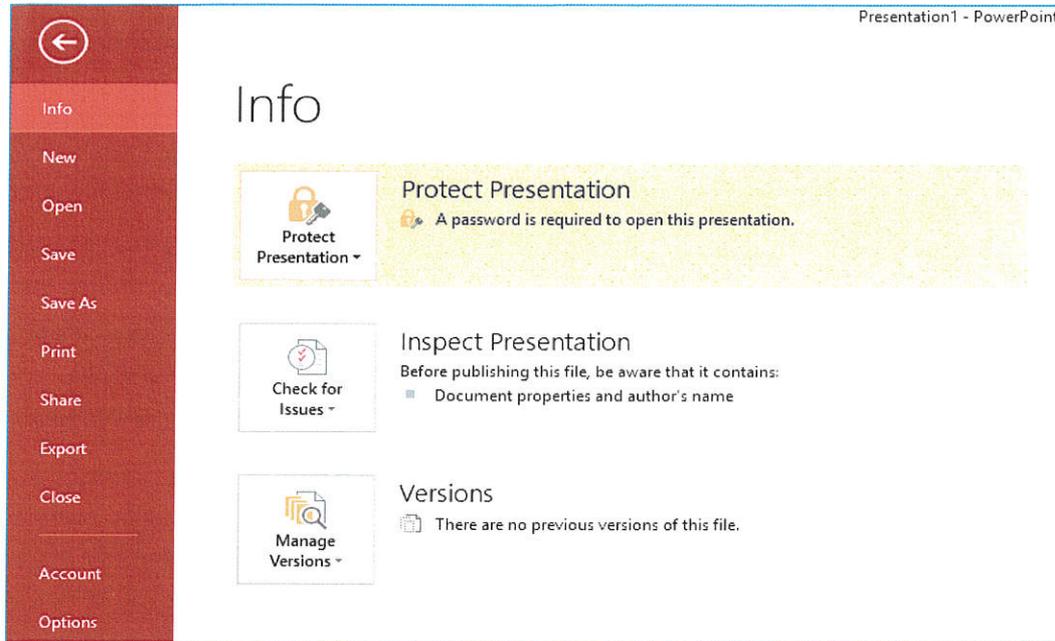
Rajah 2: Skrin paparan enkripsi persembahan

3. Masukkan kata laluan pada ruangan **'Password'**. Klik **'OK'** setelah selesai. Skrin **'Confirm Password'** akan dipaparkan bagi pengesahan kata laluan. Masukkan kata laluan yang sama dan klik **'OK'** (rujuk Rajah 3).



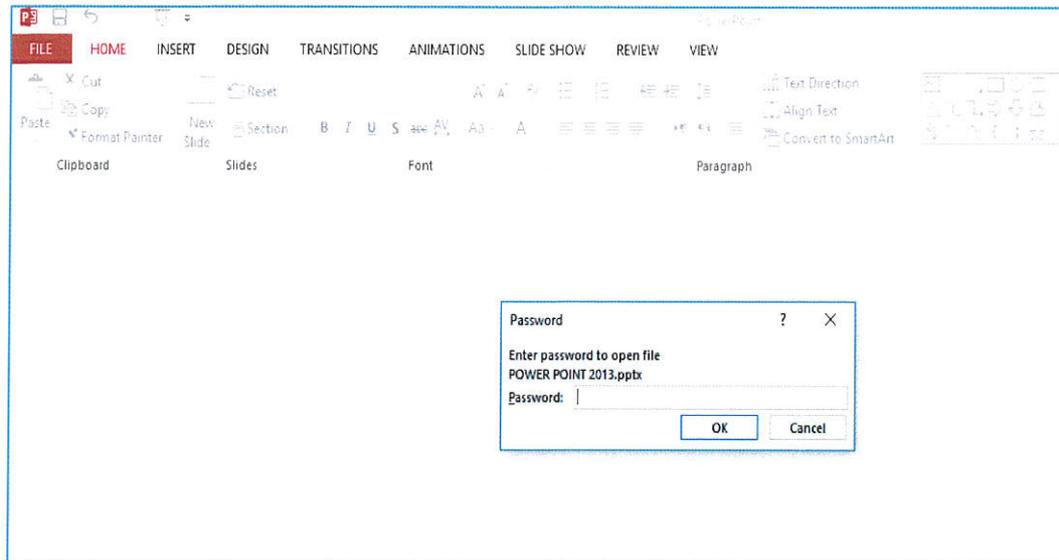
Rajah 3: Pengesahan kata laluan

4. Proses enkripsi anda selesai jika ruangan 'Protect Presentation' telah diwarnakan.



5. Seterusnya pemunya / penghantar dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.

6. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 4).



Rajah 4: Kata laluan untuk membuka dokumen

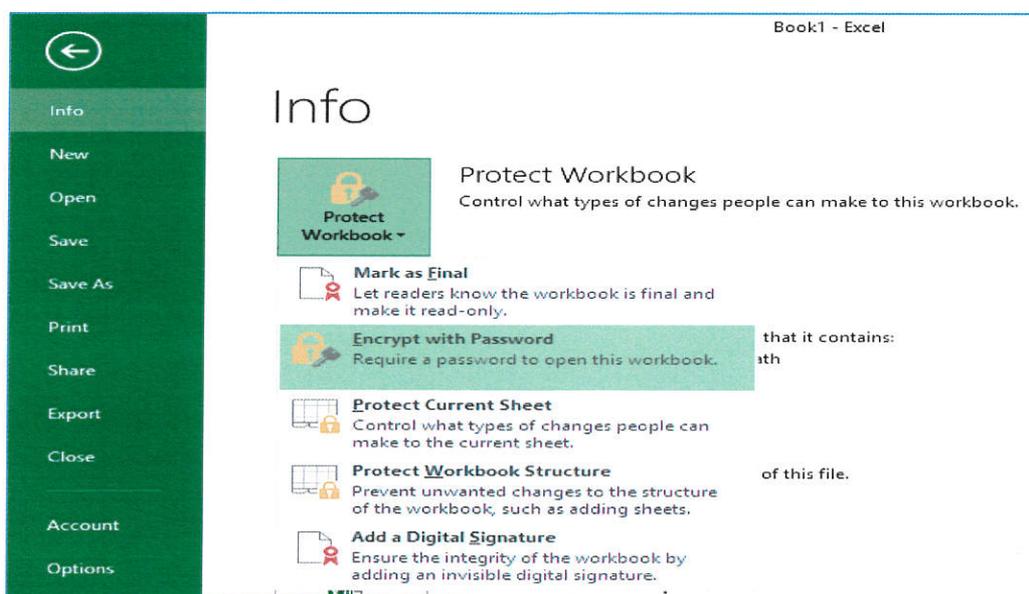
MANUAL ENKRIPSI/DEKRIPSI APLIKASI MICROSOFT EXCEL

PENGENALAN

Microsoft PowerPoint sering digunakan untuk membantu membangunkan format persembahan berdasarkan slaid. Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan pada dokumen berkaitan sebagai langkah keselamatan asas.

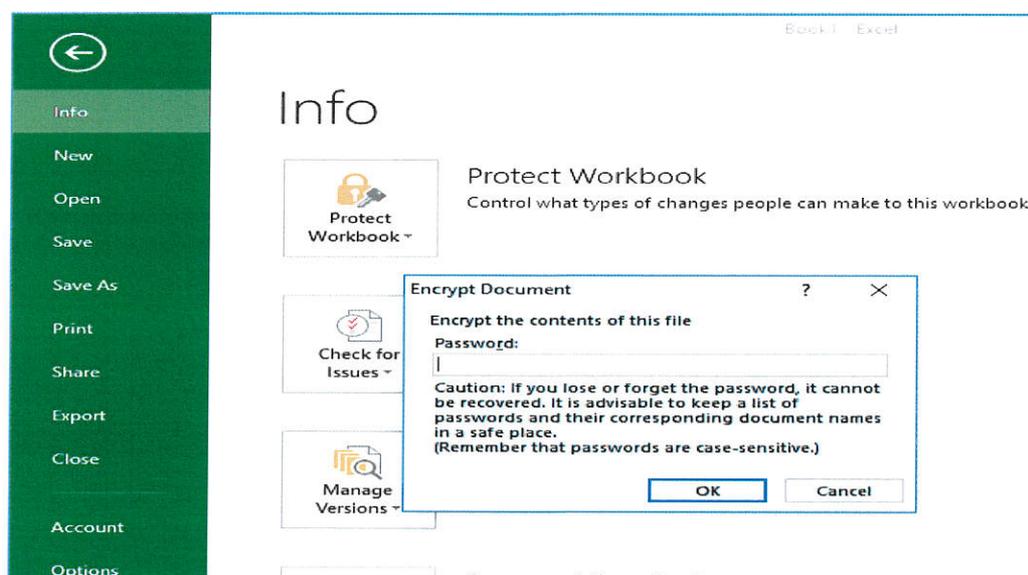
LANGKAH-LANGKAH

1. Sila klik pada menu 'FILE' dan daripada *pull-down menu* yang ditunjukkan, sila pilih 'Info' (rujuk Rajah 1). Klik 'Protect Workbook' dan pilih 'Encrypt with Password'.



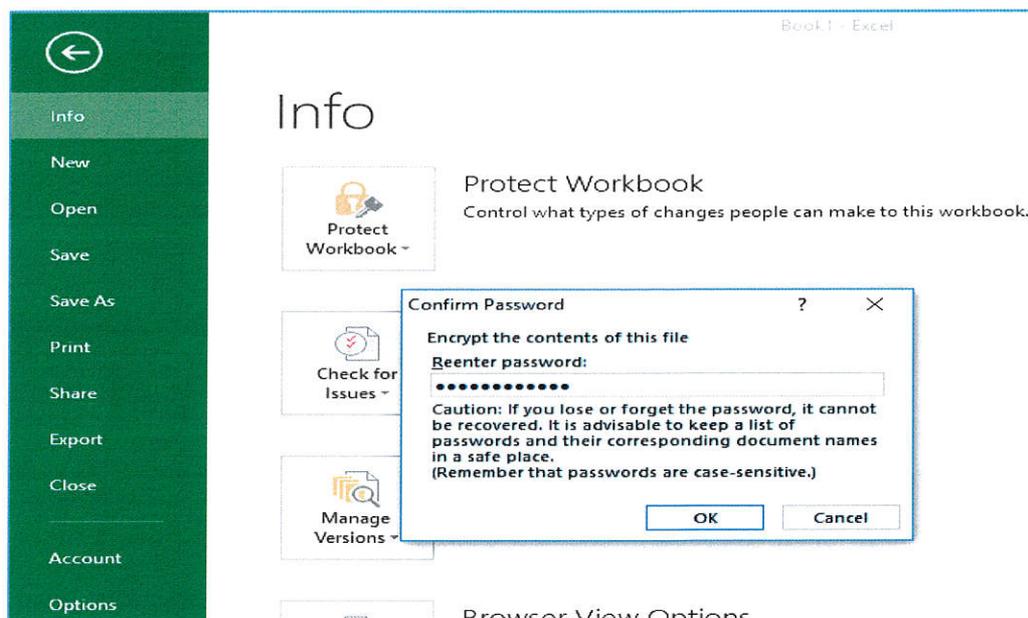
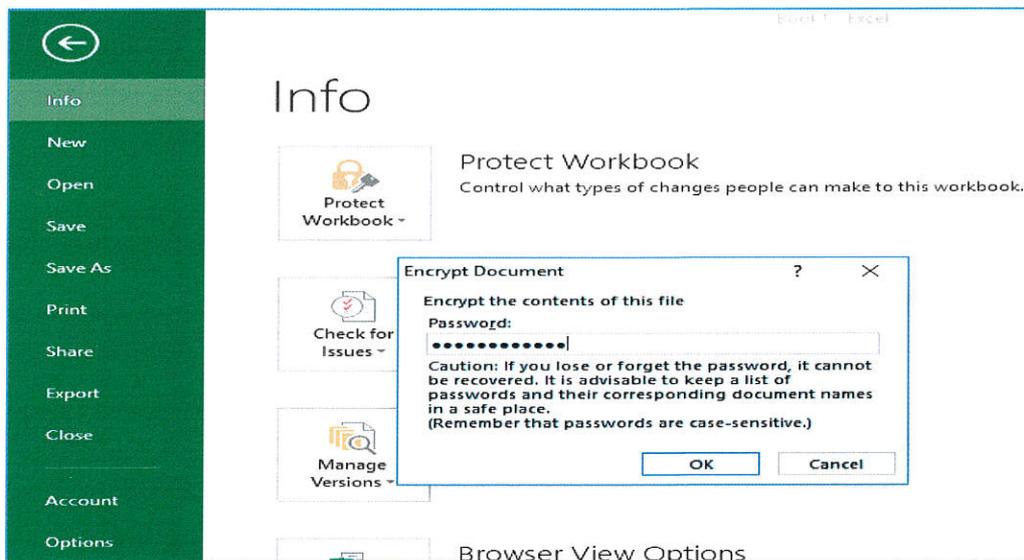
Rajah 1: Skrin *Protect Workbook*

2. Skrin berikut akan dipaparkan (rujuk Rajah 2).



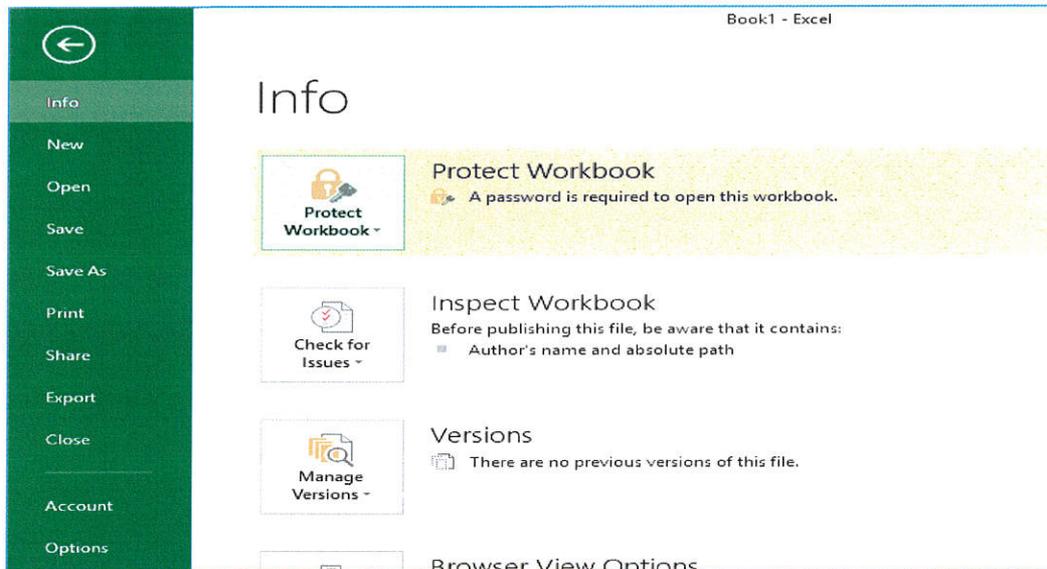
Rajah 2: Skrin paparan enkripsi dokumen

3. Masukkan kata laluan pada ruangan 'Password'. Klik 'OK' setelah selesai. Skrin 'Confirm Password' akan dipaparkan bagi pengesahan kata laluan. Masukkan kata laluan yang sama dan klik 'OK' (rujuk Rajah 3).



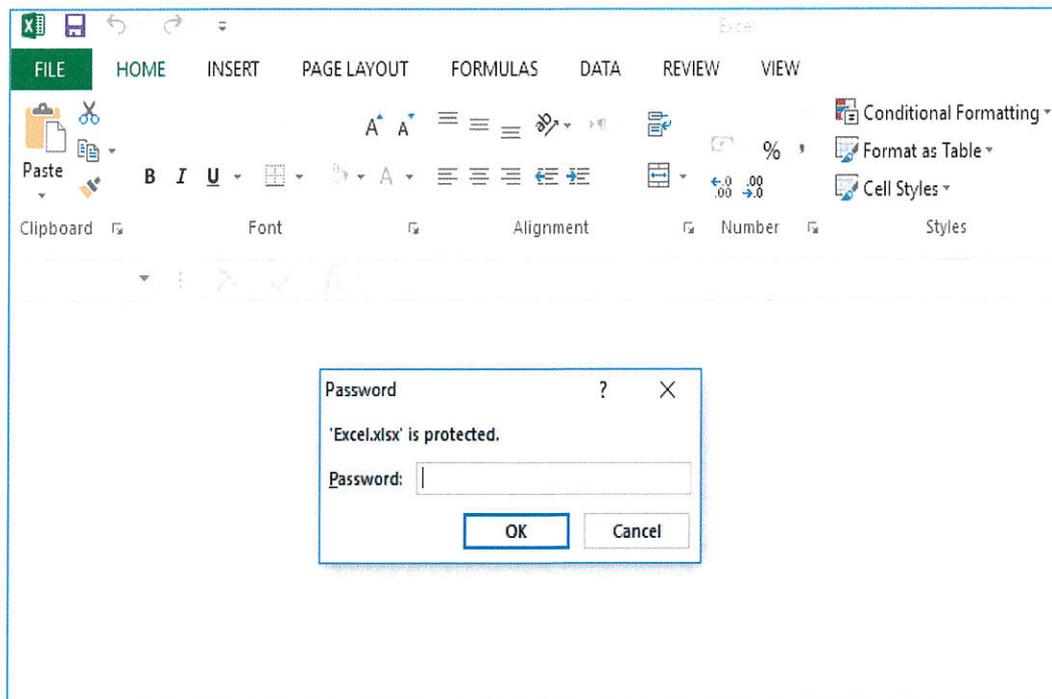
Rajah 3: Pengesahan kata laluan

4. Proses enkripsi anda selesai jika ruangan **'Protect Workbook'** telah diwarnakan.



5. Seterusnya pemunya / penghantar dokumen akan memaklumkan penerima tentang kata laluan melalui e-mel ataupun telefon bagi membuka dokumen berkenaan.

6. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh pihak lain (rujuk Rajah 4).



Rajah 4: Kata laluan untuk membuka dokumen

