GARIS PANDUAN
PENGGUNAAN DAN PENGURUSAN E-MEL RASMI
AGENSI ANTIDADAH KEBANGSAAN

Unit Keselamatan ICT
Bahagian Teknologi Maklumat dan Komunikasi

Versi 1.0
27 Jun 2019

Kandungan

1. PENGENALAN

Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. E-mel adalah digunakan untuk tujuan komunikasi rasmi dan didaftarkan di bawah agensi Kerajaan. E-mel boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

(a) E-mel Rahsia Rasmi

E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya samada *Terhad* atau *Sulit*. Maklumat *Rahsia* atau *Rahsia Besar* TIDAK boleh dihantar melalui e-mel.

(b) E-mel Bukan Rahsia Rasmi

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

Warga Agensi Antidadah Kebangsaan (AADK) diberi kemudahan e-mel rasmi mengikut kelayakan masing-masing. Setiap warga adalah bertanggungjawab kepada e-mel rasmi masing-masing dan perlu mematuhi etika seperti yang dinyatakan dalam PKPA Bil.1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik Di Agensi-agensi Kerajaan.

1.1 Tujuan

Tujuan Garis Panduan Penggunaan dan Pengurusan E-mel Rasmi AADK adalah:

(a) Menggariskan tatacara penggunaan dan pengurusan e-mel rasmi kepada semua pegawai dan kakitangan AADK;

(b) Memastikan kemudahan e-mel rasmi AADK digunakan dengan baik dan selamat;

(c) Meminimakan sebarang permasalahan berkaitan penggunaan perkhidmatan e-mel rasmi AADK.

1.2 Skop

Skop garis panduan ini meliputi:
(a) Kemudahan yang disediakan untuk pengguna e-mel rasmi AADK;
(b) Penggunaan e-mel rasmi; dan
(c) Pengurusan rekod-rekod e-mel rasmi.
(d) Tatacara Pengurusan Enkripsi/ Dekripsi Dokumen.

1.3 Pengguna

Dokumen ini disediakan khas sebagai rujukan sekaligus meningkatkan kefahaman warga AADK untuk mengamalkan penggunaan dan pengurusan e-mel secara lebih berkesan.

2. KEMUDAHAN YANG DISEDIAKAN UNTUK PENGGUNA E-MEL RASMI AADK

2.1 Hak Milik

Sistem e-mel rasmi AADK adalah diselenggara oleh Unit Keselamatan ICT (UKICT), Bahagian Teknologi Maklumat dan Komunikasi (BTMK). Semua akaun e-mel rasmi yang diwujudkan oleh UKICT untuk pegawai dan kakitangan adalah merupakan hakmilik AADK. Ia adalah kemudahan yang tertakluk kepada peraturan AADK dan boleh ditarik balik jika penggunaannya melanggar peraturan.

2.2 Tanggungjawab Pengguna

Semua pengguna adalah bertanggungjawab ke atas e-mel rasmi masing-masing. AADK tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel rasmi.

2.3 Permohonan Akaun Baru

Pentadbir E-mel akan memproses permohonan e-mel yang lengkap yang diterima secara atas talian melalui Sistem Permohonan Emel AADK. Akaun e-mel rasmi pengguna akan diwujudkan dalam tempoh dua (2) hari bekerja. Pengguna e-mel baharu mesti menukar katalaluan sementara yang diberikan selaras dengan keperluan Dasar Keselamatan ICT AADK versi yang terkini.

2.4 Saiz *Mailbox*

Setiap pengguna diberikan *mailbox* bersaiz 2048 MB (basic) atau 15 360 MB (advanced). Setiap pengguna bertanggungjawab untuk menguruskan e-mel masing-masing dengan memastikan e-mel yang disimpan tidak melebihi 90% daripada saiz *mailbox* yang telah diperuntukkan. Kapasiti *mailbox* yang tinggi (petunjuk aras *mailbox* akan bertukar daripada warna hijau kepada merah) akan menurunkan prestasi kelajuan emel pengguna.

2.5 Fungsi Mengikut Kelayakan

Akaun e-mel rasmi hanya akan diberikan kepada kakitangan yang membuat permohonan akaun e-mel rasmi AADK melalui Sistem Permohonan Emel yang boleh dicapai secara atas talian http://sistemaadk.adk.gov.my/email/

2.6 Akaun Yang Tidak Aktif

Akaun e-mel rasmi yang tidak digunakan untuk tempoh 6 bulan akan dibekukan penggunaannya dan seterusnya dihapuskan kecuali telah dimaklumkan kepada Pentadbir E-mel. Cawangan Sumber Manusia, Ibu Pejabat AADK adalah bertanggungjawab untuk memaklumkan kepada Pentadbir E-mel jika terdapat kakitangan yang telah bertukar/pencen atau berkursus/bercuti panjang melebihi 6 bulan. Capaian e-mel rasmi kakitangan yang tidak lagi berkhidmat di AADK akan dihentikan serta-merta selepas menerima pemakluman rasmi daripada Cawangan Sumber Manusia.

2.7 Pemantauan Dan Pemeriksaan Oleh Pentadbir E-mel

BTMK berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel yang sesuai untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur *spamming*.

3. PENGGUNAAN E-MEL RASMI

Warga AADK haruslah menggunakan e-mel rasmi secara bertanggungjawab berlandaskan undang-undang negara, peraturan-peraturan Perkhidmatan Awam, Dasar Keselamatan ICT (DKICT) AADK serta mematuhi etika penggunaan e-mel rasmi. Panduan dan etika penggunaan e-mel rasmi AADK yang harus diamalkan adalah seperti berikut:

(a) Memastikan penghantaran e-mel rasmi menggunakan akaun e-mel rasmi pengguna dan alamat e-mel penerima yang betul;

(b) Segala urusan rasmi adalah dilarang menggunakan alamat e-mel persendirian seperti *yahoo.com*, *gmail.com*, *streamyx.com.my* dan sebagainya;

(c) Mengutamakan penggunaan e-mel rasmi sebagai media komunikasi untuk urusan dalaman agensi atau dengan pelanggan luar;

(d) Memastikan setiap e-mel yang diterima dibalas dengan kadar segera mengikut keperluan;

(e) Memastikan sebarang mesej yang dihantar melalui e-mel tidak lagi disusuli menerusi media lain seperti faks dan surat;

(f) Memastikan setiap e-mel rasmi mempunyai tajuk yang sesuai dengan kandungan e-mel;

(g) Menggunakan bahasa dan ayat yang jelas, tepat dan mudah difahami oleh penerima e-mel;

(h) Menggunakan bahasa formal di dalam e-mel rasmi;

(i) Menggunakan kemudahan “Reply” untuk menjawab e-mel tanpa sebarang perubahan kandungan asal e-mel;

(l) Menggunakan kemudahan "Reply To All" jika jawapan perlu disalin kepada semua penerima e-mel;

(m) Tidak menggunakan kemudahan "Auto-Reply" kecuali untuk memaklumkan pegawai lain yang boleh dihubungi sekiranya pegawai berkenaan berada di luar pejabat yang tiada kemudahan Internet;

(n) Menggunakan kemudahan "Forward" untuk memanjangkan e-mel kepada penerima lain tanpa sebarang perubahan;

(o) Memastikan kemudahan "salinan kepada" (cc) jika sesuatu e-mel perlu dimaklumkan kepada penerima yang berkaitan sahaja; dan

(p) Memastikan kemudahan "blind cc" (bcc) digunakan bagi tujuan khusus dan terkawal (bukan sewenang-wenangnya).

3.1 Saiz E-mel rasmi

Saiz maksimum e-mel rasmi (termasuk kepilan) samada untuk dihantar atau diterima adalah 10 MB. Jika saiz e-mel rasmi adalah agak besar, pengguna disarankan supaya menggunakan kaedah pemampatan (*compression*) bagi mengurangkan saiz fail contohnya menggunakan perisian *WinZip*.

3.2 Enkripsi Fail Kepilan

Sebarang fail yang dihantar khususnya *Terhad* atau *Sulit* harus dilakukan enkripsi sebelum dikepilkan untuk dihantar kepada penerima bagi menjamin keselamatan dan mengelakkan kebocoran maklumat. *Microsoft Office* mempunyai fungsi "inbuilt" enkripsi masing-masing. Tatacara Pengurusan Enkripsi/ Dekripsi Dokumen adalah seperti di Lampiran A. Bagi memperketatkan lagi keselamatan penghantaran fail terenkripsi, pengguna dinasihatkan supaya memaklumkan katalaluan melalui medium yang berasingan seperti melalui telefon ataupun khidmat pesanan ringkas.

3.3 Penerimaan E-mel Tanpa Diminta (*Unsolicited Email*)

Pengguna tidak digalakkan membuka e-mel yang diterima daripada penghantar yang tidak diketahui atau diragui. Ini bagi melindungi pengguna serta aset ICT AADK daripada aktiviti yang tidak diingini seperti *phishing*, ancaman virus, *spamming*, dan lain-lain *malware*. Pentadbir E-mel hendaklah dimaklumkan segera sekiranya pengguna mengesyaki terdapat kebarangkalian akaun e-mel pengguna telah dikompromi.

3.4 Mengenalpasti Identiti Pengguna

Pengguna perlu mengenalpasti dan mengesahkan identiti pihak yang berkomunikasi dengannya sebelum meneruskan komunikasi dan transaksi maklumat melalui e-mel. Ini bertujuan untuk melindungi maklumat Kerajaan daripada sebarang bentuk penyalahgunaan.

3.5 Katalaluan

Katalaluan adalah rahsia dan tidak boleh didedahkan kepada orang lain. Pengguna disarankan untuk menggunakan katalaluan kukuh yang mempunyai ciri-ciri berikut:

(a) Kataluan mestilah sekurang-kurangnya terdiri daripada 12 aksara dan pengguna dinasihatkan menggunakan kombinasi *alphanumeric* dan simbol. (contoh: a@dk1buPejabat19).

(b) Pengguna dilarang menggunakan katalaluan yang sama dengan akaun e-mel rasmi (id pengguna) untuk mengelakkan tekaan kata laluan oleh pengguna hasad.

3.6 Perkara Yang Dilarang Dalam Penggunaan E-mel

Pengguna adalah dilarang daripada melakukan sebarang aktiviti berikut:-

(a) Menggunakan e-mel rasmi untuk menghantar dokumen/ kepilan yang menyalahi undang-undang seperti bahan lucah, perjudian, jenayah, cetak rompak atau apa-apa maklumat yang menjejaskan reputasi AADK dan Perkhidmatan Awam;

(b) Menggunakan e-mel rasmi untuk tujuan peribadi, komersial atau politik;

(c) Menghantar e-mel sampah (*junk mail*) dan e-mel *spam*;

(d) Menyebarkan kod perosak seperti *virus*, *worm*, dan *trojan horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

(e) Menyimpan dan memuat turun bahan yang mempunyai hakcipta, termasuk yang dimuat turun dari Internet ke dalam sistem e-mel rasmi AADK atau menyebarkan kepada pihak lain tanpa mendapat kebenaran terlebih dahulu daripada pemilik hakcipta yang berkenaan;

(f) Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akses akaun kepada orang lain untuk menjawab e-mel rasmi bagi pihaknya; dan

(g) Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah.

4. PENGURUSAN REKOD-REKOD E-MEL RASMI

Rekod elektronik rasmi adalah merupakan rekod awam mengikut tafsiran Akta Arkib Negara Malaysia No. 44/1996. Ia merangkumi sebarang mesej atau rekod komputer (termasuk fail kepilan) yang diwujud, dihantar, diserah, dijawab, diedar, disimpan, disalin, dipapar, dibaca atau dicetak oleh sistem atau perkhidmatan sesebuah agensi kerajaan. Rekod awam merupakan sumber strategik dan bahan bukti yang perlu diurus secara terkawal, sistematik dan cekap.

4.1 Penyimpanan Rekod-Rekod E-mel

Pengguna hendaklah mengurus dan memastikan jumlah e-mel yang disimpan di dalam *mailbox* adalah tidak melebihi 90% daripada ruang storan yang telah diperuntukkan dan mengutamakan penyimpanan e-mel mengikut keperluan sahaja. Pengguna disarankan supaya mewujudkan *sub folder* mengikut subjek terutamanya bagi *folder Inbox* dan *folder Sent* untuk menyimpan e-mel bagi memudahkan carian.

4.2 Mencetak dan Memfail Rekod E-mel

Rekod e-mel berkaitan sesuatu keputusan penting atau tindakan yang telah diambil boleh dicetak dan difailkan sekiranya terdapat keperluan sahaja.

4.3 Penghapusan Rekod E-mel

Pengguna hendaklah menghapuskan sebarang e-mel berunsurkan *spam* yang berkemungkinan mempunyai virus. Lain-lain e-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan serta tidak diperlukan lagi perlu dihapuskan.

5. TANGGUNGJAWAB PENGGUNA

Garis Panduan Penggunaan dan Pengurusan E-Mel Rasmi AADK ini menggariskan tatacara penggunaan dan pengurusan rekod-rekod e-mel rasmi AADK untuk dijadikan rujukan dan panduan kepada warga AADK.

6. KHIDMAT NASIHAT

Sebarang kemusykilan yang timbul berkaitan dengan garis panduan ini hendaklah dirujuk kepada:-

Unit Keselamatan ICT
Bahagian Teknologi Maklumat dan Komunikasi
Agensi Antidadah Kebangsaan
Aras 3, Blok A,
Jalan Maktab Perguruan Islam,
43000 Kajang, Selangor

Tel: 03-89112357/2349
E-mel: ukict@adk.gov.my

RUJUKAN:

1. Surat Arahan Ketua Pengarah MAMPU rujukan MAMPU.BDPICT.700-2/36(1): “Pemantapan Penggunaan dan Pengurusan E-mel di Agensi-Agensi Kerajaan” – MAMPU, 1 Julai 2010.

2. Surat Arahan Ketua Pengarah MAMPU rujukan UPTM159/526/9 Jld.4 (60) : “Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan” – MAMPU, 23 Nov 2007.

3. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : “Garis Panduan Mengenai Tatacara Penggunaan Internet Dan E-mel Di Agensi-Agensi Kerajaan” – MAMPU, 2003.

4. “*Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS)” – MAMPU, 15 Januari 2002.

5. Garis Panduan Pengurusan Rekod Elektronik: Pengurusan Rekod Elektronik dalam Persekitaran Tidak Berstruktur – Arkib Negara Malaysia, 2003.

6. Rekod Elektronik dan Akta Arkib Negara 2003 – Arkib Negara Malaysia, 2003.

7. Dasar Pengurusan Rekod dan Arkib Elektronik – Arkib Negara Malaysia, 2003.

8. Dasar Keselamatan ICT (DKICT) Agensi Antidadah Kebangsaan (Versi 4.1) – AADK, 2018.

GLOSARI

Warga AADK	Semua kakitangan Agensi Antidadah Kebangsaan (AADK)
Pengguna	Semua kakitangan AADK yang menggunakan perkhidmatan e-mel rasmi AADK.
Pentadbir E-mel	Dikendalikan oleh Unit Keselamatan ICT, BTMK.
E-mel	Satu kaedah mengarang, menghantar, menyimpan dan menerima mesej melalui sistem komunikasi elektronik.
E-mel rasmi	E-mel rasmi adalah merupakan rekod maklumat yang dihasilkan, diterima atau disimpan secara rasmi dengan menggunakan kemudahan elektronik, yang juga tertakluk kepada penafsiran Rekod Awam. Ini bermaksud mesej e-mel tersebut adalah merupakan maklumat-maklumat atau rekod-rekod yang dihasilkan atau diterima oleh pegawai dan kakitangan AADK di dalam melaksanakan tugas-tugas rasmi mereka, dan ianya mempunyai kepentingan sebagai bahan bukti kepada sesuatu transaksi itu.
E-mel tidak rasmi	E-mel tidak rasmi adalah merupakan rekod e-mel yang dihasilkan, diterima atau disimpan atas urusan peribadi yang dibenarkan oleh AADK. Ianya tidak mempunyai kaitan langsung dengan tugas-tugas rasmi yang dijalankan oleh pegawai dan kakitangan AADK.
Mailbox	Peti mail pengguna untuk menyimpan semua e-mel yang diterima dan dihantar pengguna.
Rekod	Bahan dalam bentuk bertulis atau bentuk lain yang menyatakan fakta atau peristiwa atau selainnya merakamkan maklumat termasuklah kertas, dokumen, daftar, bahan bercetak, buku, peta, pelan, lukisan, gambar foto, mikrofilem, filem sinematograf, rakaman bunyi, rekod yang dihasilkan secara elektronik, tanpa mengira bentuk atau ciri-ciri fizikal dan apa-apa salinannya.

Rekod Elektronik	Rekod dalam bentuk elektronik atau berdigit yang diwujudkan, ditawan, diselenggarakan atau disimpan semasa menjalankan fungsi Kerajaan selaras dengan takrif rekod yang diberikan dalam Akta Arkib Negara 2003. Ini termasuk tetapi tidak terhad kepada kertas, dokumen, daftar, bahan bermaklumat, buku, peta, pelan, lukisan, gambar foto dan rakaman bunyi dalam bentuk elektronik atau berdigit.
Rekod E-mel	Sebarang mesej atau rekod komputer yang wujud, dihantar, diserah, dijawab, diedar, disimpan, disalin, dipapar, dibaca atau dicetak oleh sistem/perkhidmatan yang menepati istilah Rekod Awam di dalam Akta Arkib Negara 2003.
Rekod Awam	Rekod yang diterima secara rasmi atau yang dikeluarkan oleh mana-mana pejabat awam bagi perjalanan hal ehwalnya atau oleh mana-mana pekhidmat awam atau pekerja pejabat awam dalam perjalanan tugas rasminya dan termasuk rekod mana-mana perusahaan Kerajaan dan juga termasuk segala rekod yang, pada permulaan kuat kuasa Akta ini, adalah dalam jagaan atau di bawah kawalan Arkib Negara Malaysia.

TATACARA PENGURUSAN ENKRIPSI/ DEKRIPSI DOKUMEN

1. PENGENALAN

Manual pengguna ini dihasilkan bagi menerangkan tatacara enkripsi / dekripsi yang boleh dilakukan pada dokumen berkaitan (Microsoft Office Word, Excel dan Power Point sahaja) sebagai langkah keselamatan asas ketika melibatkan penghantaran dokumen terperingkat melalui e-mel rasmi AADK.

2. LATAR BELAKANG

Warga AADK haruslah menggunakan e-mel rasmi AADK secara bertanggungjawab berlandaskan peraturan-peraturan Perkhidmatan Awam dan Dasar Keselamatan ICT (DKICT) AADK yang terkini. Sebarang dokumen yang diklasifikasikan sebagai dokumen terperingkat harus dienkripsi sebelum dikepilkan untuk dihantar kepada penerima e-mel bagi menjamin keselamatan dan mengelakkan kebocoran maklumat semasa transaksi maklumat.

3. TANGGUNGJAWAB PENGGUNA

a) Pemunya dokumen dinasihatkan supaya memaklumkan kata laluan kepada penerima dokumen melalui medium yang berasingan seperti telefon.

b) Warga AADK adalah bertanggungjawab sepenuhnya sebagai pemilik dokumen ke atas pengurusan dan penetapan katalaluan pada dokumen terenkripsi masing-masing.
(Nota: Bahagian Teknologi Maklumat dan Komunikasi (BTMK) AADK tidak akan bertanggungjawab ke atas sebarang masalah lupa kata laluan yang ditetapkan ketika proses enkripsi dokumen)

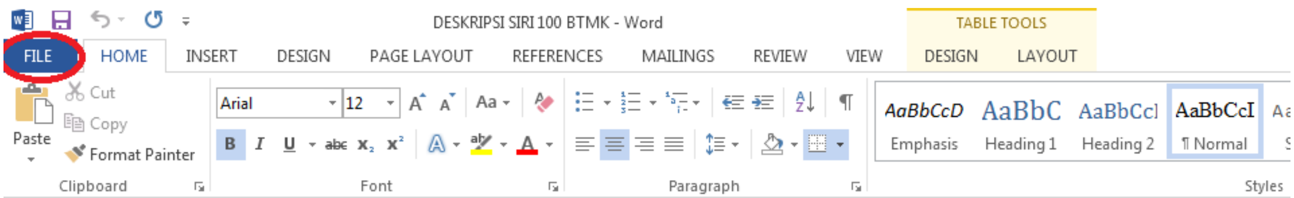
c) Pemilihan kata laluan yang kukuh semasa proses enkripsi dokumen perlu mematuhi Dasar Keselamatan ICT AADK yang terkini iaitu :
   - ✓ Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara (contoh: a, b, c), angka (contoh: 1, 2, 3) dan aksara khusus (contoh: @, !, #).

MANUAL PENGGUNA

SEKSYEN 1: ENKRIPSI DOKUMEN.

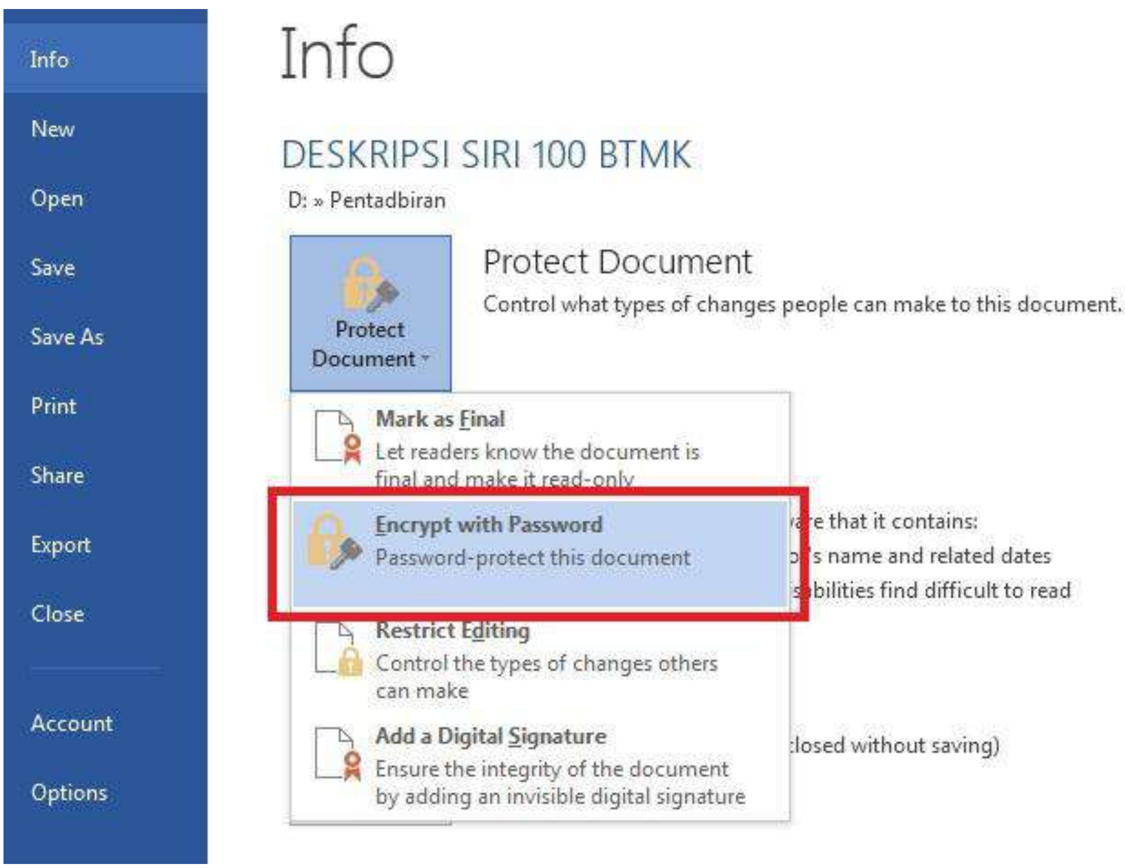
MICROSOFT WORD

1. Buka dokumen (.docx) yang hendak dienkrip (paparan di bawah adalah untuk Microsoft Office Word 2013) dan klik **File** seperti di Rajah 1**.**



Rajah 1: Paparan dokumen (Microsoft Office Word 2013).

2. Klik ***Info>Protect Document*** dan pilih ***Encrypt with Password*** daripada *drop-down menu* seperti di Rajah 2.



Rajah 2: Enkripsi dokumen dalam Microsoft Word.

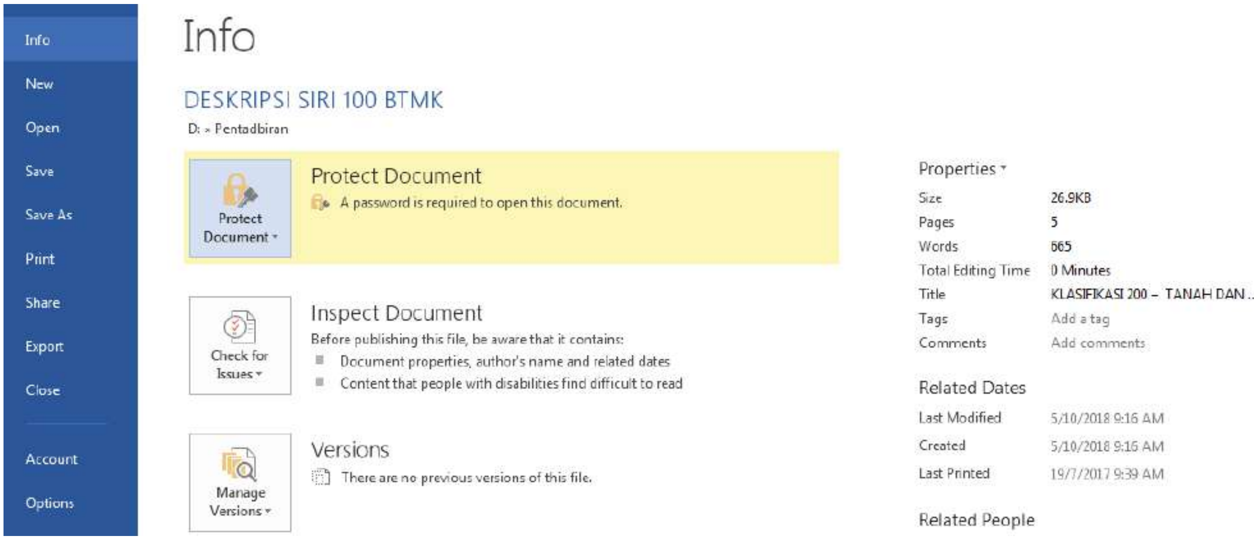
3. Masukkan kata laluan yang sesuai dan kukuh selaras dengan pematuhan Dasar Keselamatan ICT AADK pada ruangan *Password* dan klik butang **OK** setelah selesai*.
*Mesej *caution* yang dipaparkan seperti Rajah 3 adalah berkaitan dengan Tatacara Pengurusan Enkripsi/ Dekripsi Dokumen - Bahagian 3 (b) Tanggungjawab Pengguna seperti yang telah dinyatakan di atas.

Rajah 3: Penetapan kata laluan untuk enkripsi dokumen.

4. Masukkan kata laluan yang sama pada *pop-up* mesej pengesahan kata laluan di ruangan *Reenter password* seperti yang dipaparkan dalam Rajah 4 dan klik butang **OK** setelah selesai.

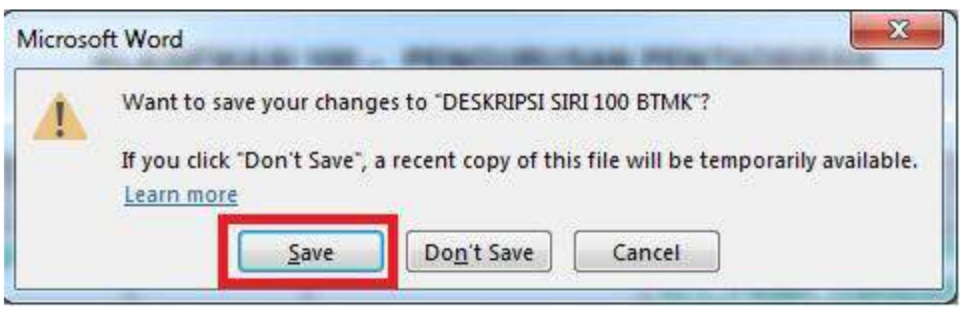
Rajah 4: Pengesahan kata laluan yang telah dimasukkan.

5. Seterusnya, perubahan warna pada butang ***Protect Document*** di tab ***Info*** seperti Rajah 5 merupakan indikator bahawa proses penetapan kata laluan telah berjaya dilaksanakan.



Rajah 5: Perubahan warna fungsi ***Protect Document*** selepas pelaksanaan enkripsi.

6. Sila klik butang ***Save*** seperti di Rajah 6. Ini bagi memastikan proses enkripsi dokumen dilaksanakan dengan sempurna.

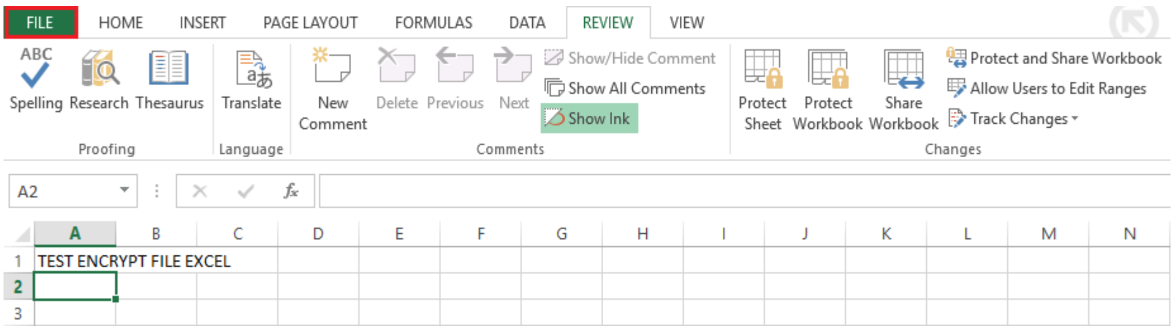


Rajah 6: Paparan pengesahan penyimpanan dokumen *(save).*

7. Dokumen tersebut kini boleh diedarkan secara elektronik melalui e-mel rasmi AADK. Pemunya dokumen perlu memaklumkan penerima dokumen tentang kata laluan melalui medium yang berasingan e.g telefon bagi membuka dokumen berkenaan.

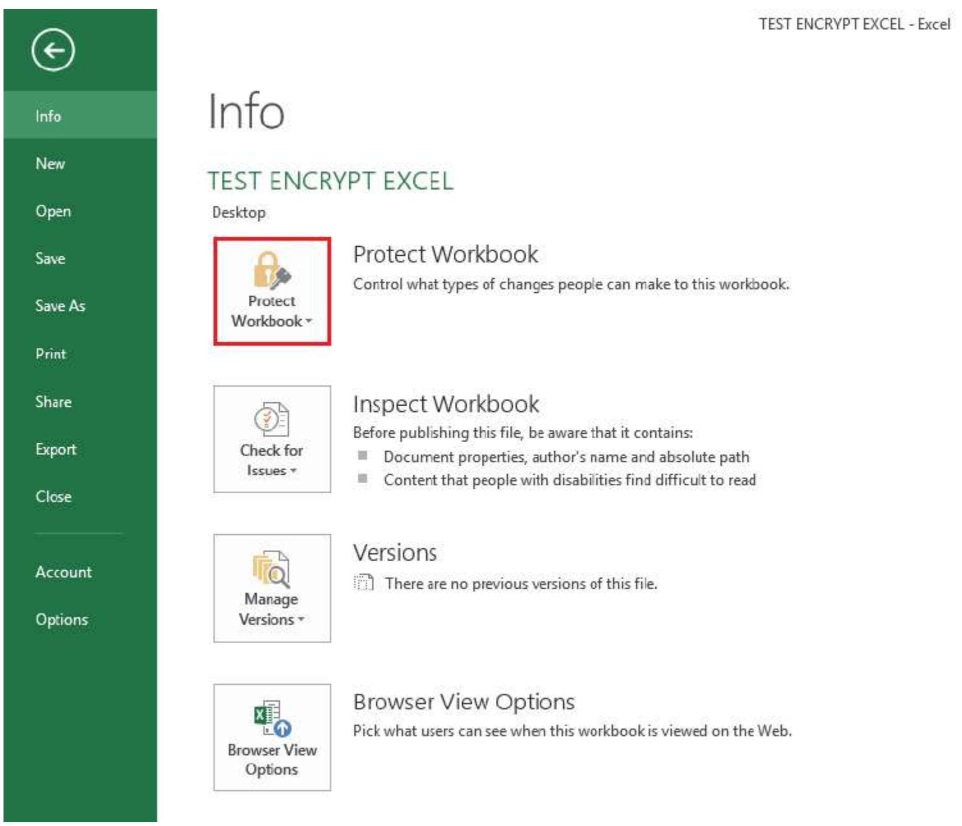
MICROSOFT EXCEL

1. Pada paparan menu, klik **File** seperti Rajah 1.



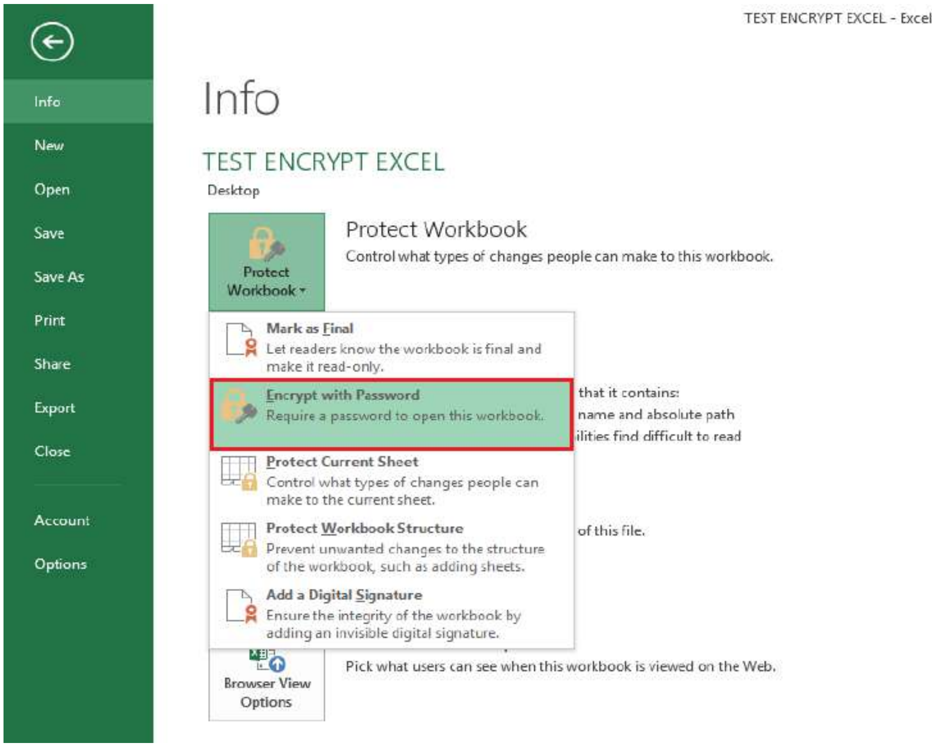
Rajah 1: Paparan dokumen (Microsoft Office Excel 2013).

2. Pada **menu Info**, klik pada butang ***Protect Workbook.***



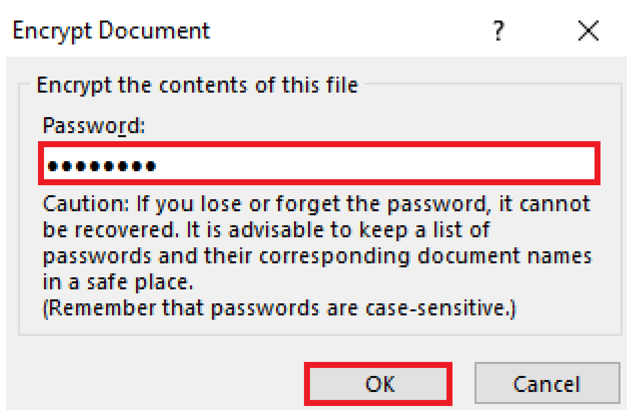
Rajah 2: Paparan dokumen – *Protect Workbook* dalam Microsoft Excel.

3. *Drop-down* **menu** ***Protect Workbook*** akan dipaparkan seperti Rajah 3, klik pada ***Encrypt with Password.***



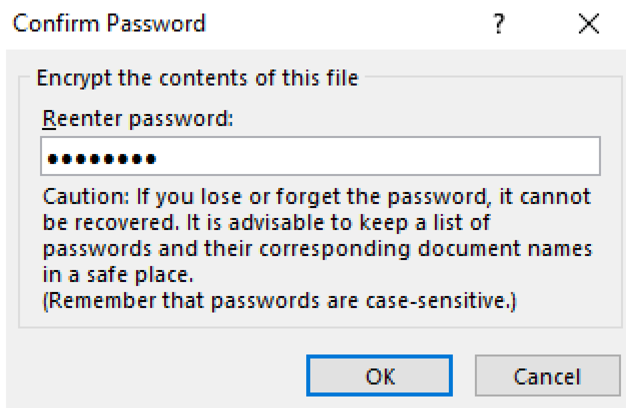
Rajah 3: Enkripsi dokumen dalam Microsoft Excel.

4. Masukkan kata laluan yang sesuai dan kukuh selaras dengan pematuhan Dasar Keselamatan ICT AADK pada ruangan *Password* dan klik butang **OK.**



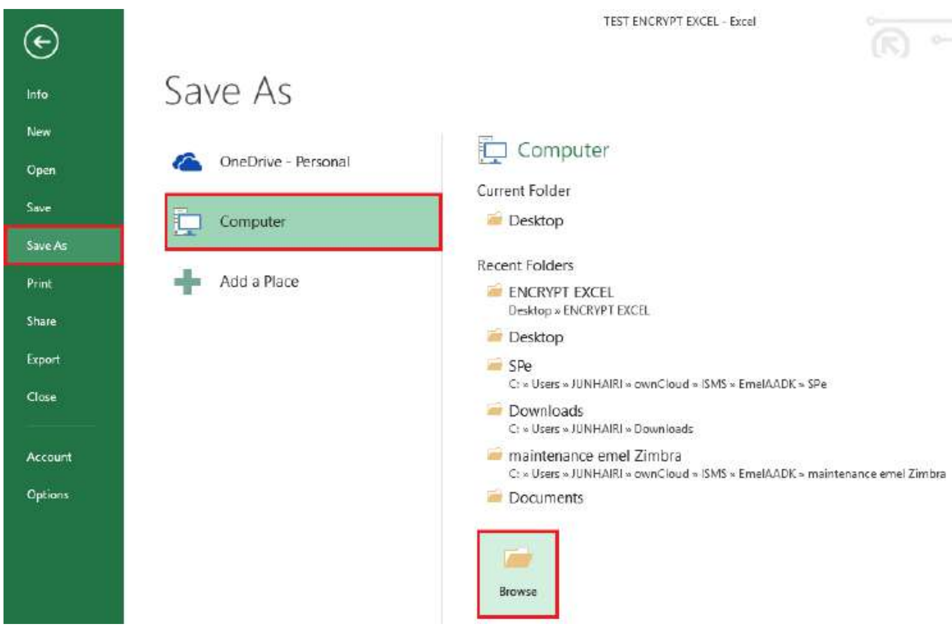
Rajah 4: Penetapan kata laluan untuk enkripsi dokumen.

5. Masukkan kata laluan yang sama pada pop-up mesej pengesahan kata laluan di ruangan Reenter password seperti yang dipaparkan dalam Rajah 5 dan klik butang **OK.**



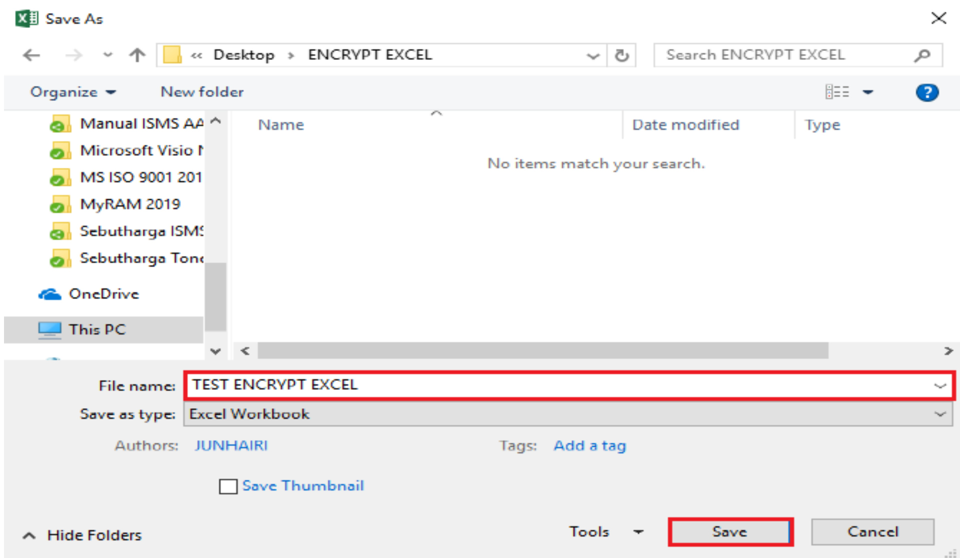
Rajah 5: Pengesahan kata laluan yang telah dimasukkan.

6. Seterusnya, klik menu **Save As** seperti Rajah 6. Klik ***Computer*** dan ikon ***Browse*** di mana fail tersebut hendak disimpan.



Rajah 6: Paparan penyimpanan dokumen.

7. Pada menu **Save As** seperti Rajah 7, tetapkan nama fail dan lokasi di mana fail tersebut hendak disimpan dan klik butang **Save**.



Rajah 7: Paparan penetapan nama fail dan lokasi penyimpanan fail .xlsx.

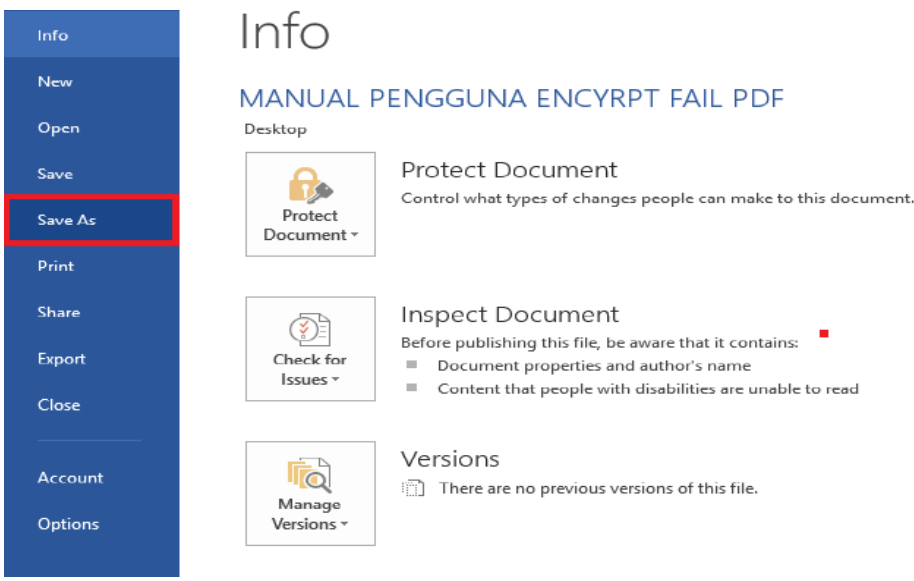
8. Dokumen tersebut kini boleh diedarkan secara elektronik melalui e-mel rasmi AADK. Pemunya dokumen perlu memaklumkan penerima dokumen tentang kata laluan melalui medium yang berasingan e.g telefon bagi membuka dokumen berkenaan.

WORD FILE KE PDF DENGAN FUNGSI *ENCRYPTION*

1. Untuk menyimpan dokumen dalam format PDF File menggunakan Microsoft Office Word 2013, klik **File** seperti Rajah 1.

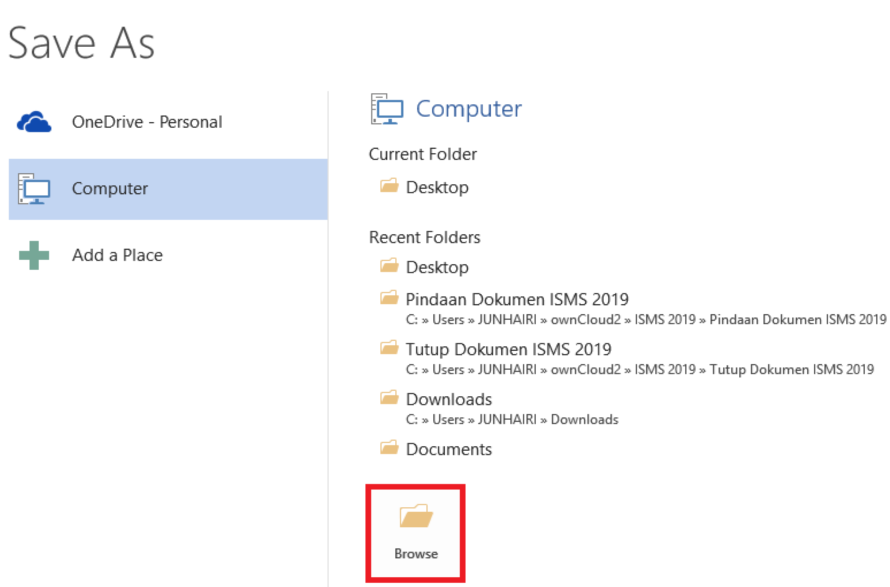
Rajah 1: Paparan dokumen (Microsoft Office Word 2013).

2. Pada paparan menu di Rajah 2, klik **Save As.**



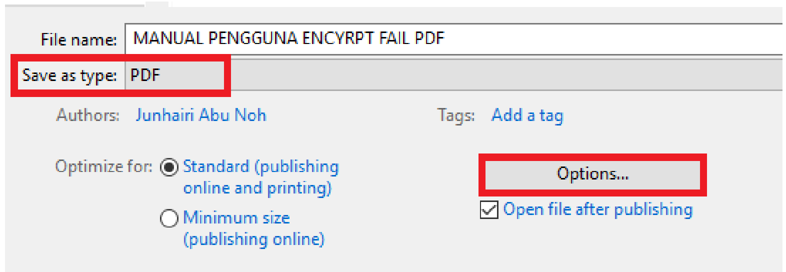
Rajah 2: Paparan *Save As* dokumen dalam Microsoft Word.

3. Paparan seperti Rajah 3 akan dipaparkan. Klik ikon **Browse.**



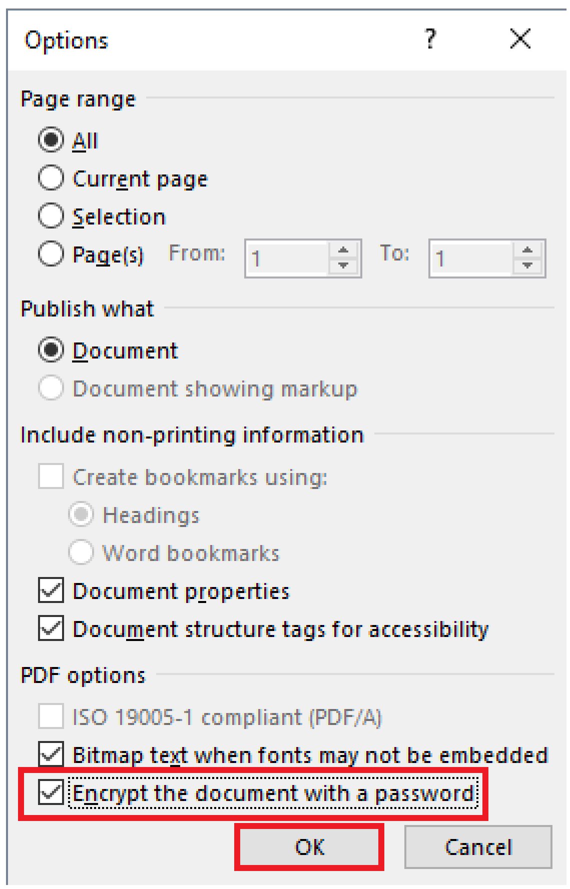
Rajah 3: *Browse* Dokumen.

4. Isikan ruangan **File name** dengan nama dokumen yang dikehendaki seperti Rajah 4. Seterusnya, pada ruangan **Save as type, pilih PDF** daripada *drop-down menu* yang dipaparkan dan klik butang **Options.**



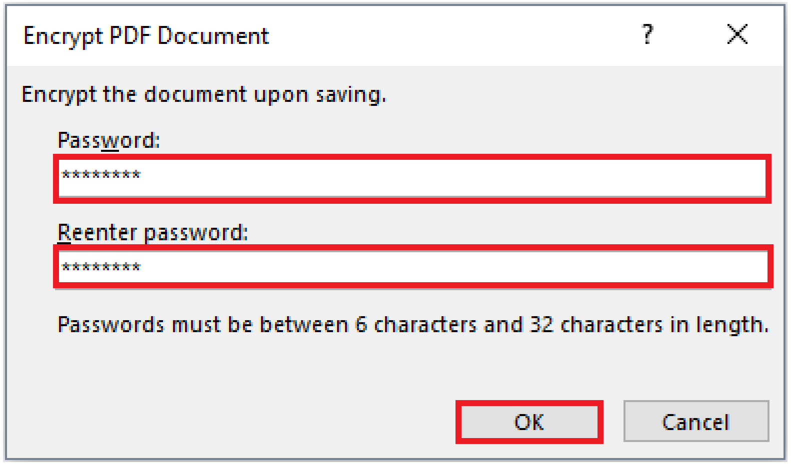
Rajah 4: Penyimpanan fail .docx ke format .pdf.

5. Pada *pop-up* menu *Options* di Rajah 5, tick *pada* ***Encrypt the document with a password*** dan klik butang **OK.**



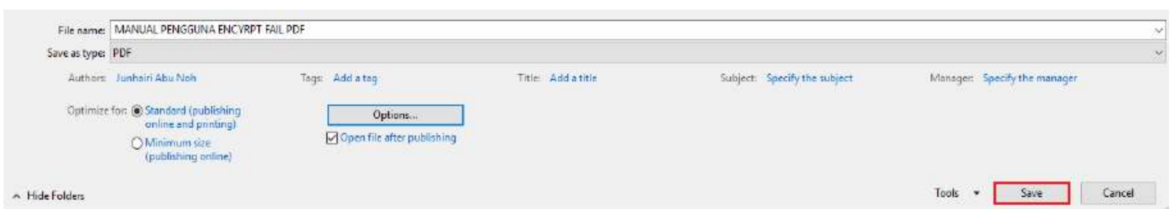
Rajah 5: Paparan menu Options.

6. **Daftar masuk kata laluan** di ruangan *Password* dan **ulang semula kata laluan** di ruangan *Reenter password*. Seterusnya, klik butang **OK** seperti Rajah 6.



Rajah 6: Penetapan kata laluan untuk proses enkripsi dokumen.

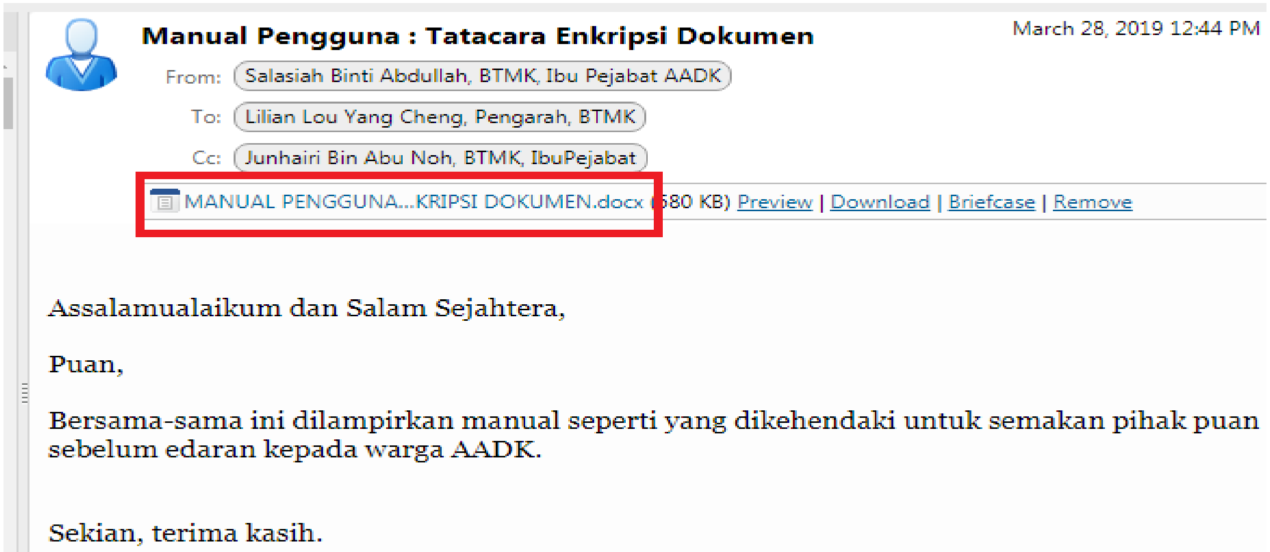
7. Rajah 7 akan dipaparkan. Pastikan klik butang ***Save*** untuk menyimpan dokumen tersebut.



Rajah 7: Paparan Penyimpanan Dokumen *(Save).*

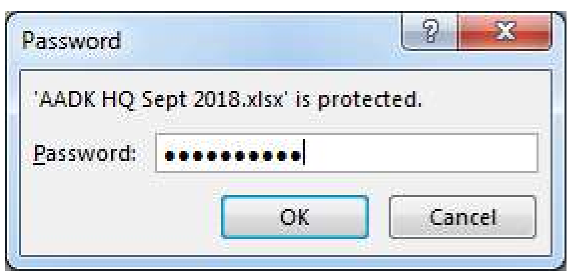
SEKSYEN 2: DEKRIPSI DOKUMEN.

1. Penerima dokumen perlu klik pada dokumen yang dilampirkan dalam e-mel seperti Rajah 1.



Rajah 1: Paparan Antarmuka E-mel Pengguna.

2. Mesej seperti Rajah 2 akan dipaparkan. Penerima dokumen perlu memasukkan kata laluan yang diterima daripada pemunya dokumen (melalui medium berasingan) sebelum mengakses dokumen tersebut.



Rajah 2: Keperluan kemasukan kata laluan untuk dekripsi dokumen.

3. Dokumen tersebut kini boleh diakses oleh penerima dokumen.

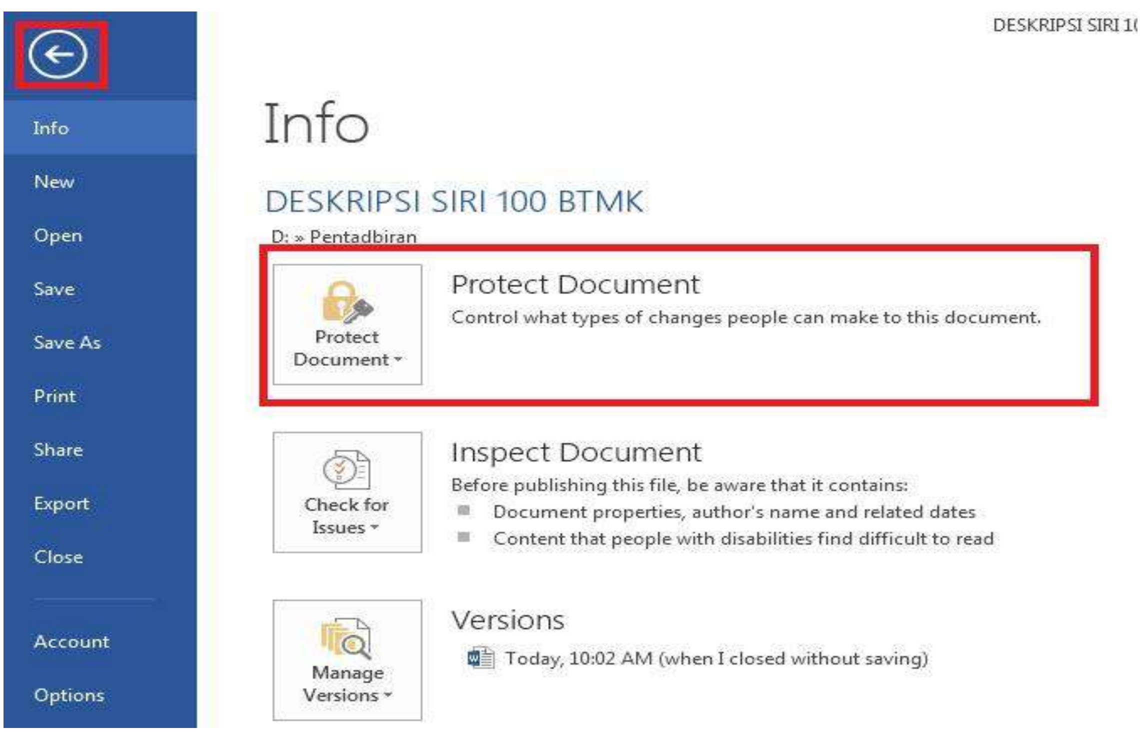
SEKSYEN 3: PEMBATALAN ENKRIPSI DOKUMEN.

1. Pembatalan kata laluan pada dokumen terenkripsi boleh dilakukan dengan mengulang langkah 1 dan 2 (SEKSYEN 1: Enkripsi Dokumen – Microsoft Word).

2. Mansuhkan (***delete***) kata laluan yang telah dimasukkan (kata laluan dipaparkan sebagai simbol titik) seperti Rajah 1 dan klik butang Ok.

Rajah 1: Pemansuhan kata laluan yang telah ditetapkan untuk proses dekripsi.

3. Perubahan warna Fungsi ***Protect Document*** kepada warna asal seperti fungsi yang lain menandakan bahawa proses dekripsi telah berjaya dilaksanakan. Untuk meneruskan proses, klik butang



Rajah 2: Pengesahan dekripsi yang telah dilaksanakan.

4. Akhir sekali, klik butang ***Save*** setelah perubahan dokumen selesai dilakukan. Ini bagi memastikan proses pembatalan enkripsi dokumen berjaya dilaksanakan.