

GARIS PANDUAN PENGUNAAN E-MEL KEMENTERIAN PERTAHANAN

BAHAGIAN PENGURUSAN MAKLUMAT
KEMENTERIAN PERTAHANAN MALAYSIA

VERSI 1.0

KANDUNGAN

1.	TAJUK.....	2
2.	TUJUAN.....	2
3.	LATAR BELAKANG	2
4.	RASIONAL.....	3
5.	TANGGUNGJAWAB PENYEDIA PERKHIDMATAN E-MEL	3
6.	PENGURUSAN REKOD-REKOD E-MEL.....	8
7.	PENGURUSAN KATA LALUAN E-MEL.....	9
8.	PROSES PERMOHONAN E-MEL.....	11
9.	PENGGUNAAN PERTAMA KALI.....	13
10.	TANGGUNGJAWAB PENGGUNA.....	14
11.	MEJA BANTUAN.....	14
	RUJUKAN.....	15
	GLOSARI.....	16
	LAMPIRAN A	
	PANDUAN ENKRIPSI / DEKRIPSI MICROSOFT OFFICE 2013.....	19
	LAMPIRAN B	
	PANDUAN ENKRIPSI DOKUMEN FORMAT PDF.....	23
	LAMPIRAN C	
	PANDUAN ENKRIPSI MENERUSI PROGRAM PEMAMPATAN.....	26
	LAMPIRAN D	
	PANDUAN PENGURUSAN ARCHIVING E-MEL.....	30

1. TAJUK

Garis Panduan Penggunaan E-mel Kementerian Pertahanan Malaysia.

2. TUJUAN

Penyediaan Garis Panduan Penggunaan E-mel Kementerian Pertahanan Malaysia adalah untuk:

- i. Menerangkan dengan lebih terperinci tatacara penggunaan dan pengurusan e-mel kepada semua pegawai dan kakitangan Kementerian Pertahanan;
- ii. Memastikan kemudahan e-mel Kementerian Pertahanan digunakan dengan baik dan selamat; dan
- iii. Meminimalkan sebarang permasalahan berkaitan penggunaan perkhidmatan e-mel.

Dokumen ini disediakan khas untuk rujukan dan kegunaan warga Kementerian Pertahanan supaya lebih memahami dan seterusnya mengamalkan penggunaan dan pengurusan e-mel yang baik dan efisien.

3. LATAR BELAKANG

Kerajaan sentiasa berusaha meningkatkan kecekapan dalam proses komunikasi di kalangan anggota-anggotanya dan juga di antara agensi Kerajaan dengan swasta dan orang ramai. Penggunaan teknologi maklumat dan komunikasi (ICT) telah membuka peluang kepada komunikasi yang lebih cepat dan mudah. Salah satu kaedah komunikasi yang semakin luas penggunaannya dalam sektor awam ialah Internet dan mel elektronik (e-mel). Selain daripada memudah dan mempercepatkan komunikasi, kaedah ini dapat mengurangkan penggunaan kertas dan akhirnya menyumbang kepada peningkatan produktiviti dan kualiti perkhidmatan.

4. RASIONAL

Setiap pegawai dan kakitangan Kementerian Pertahanan yang memohon akan mendapat satu e-mel rasmi yang digunakan untuk tujuan rasmi. Salah satu contoh alamat e-mel rasmi ialah pentadbiremel@mod.gov.my. Penggunaan e-mel rasmi boleh dikategorikan kepada dua iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

i. **E-mel Rahsia Rasmi**

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

ii. **E-mel Bukan Rahsia Rasmi**

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

Oleh itu, Bahagian Pengurusan Maklumat (BPM) telah dipertanggungjawabkan untuk membekalkan kemudahan komunikasi e-mel rasmi kepada semua pegawai dan kakitangan Kementerian Pertahanan.

5. TANGGUNGJAWAB PENYEDIA PERKHIDMATAN E-MEL

Bahagian Pengurusan Maklumat (BPM) bertanggungjawab ke atas e-mel rasmi Kementerian Pertahanan dalam aspek pelaksanaan, penggunaan dan pemantauan.

Semua Pegawai dan kakitangan yang telah disediakan kemudahan komunikasi e-mel rasmi adalah tertakluk kepada Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT) Kementerian Pertahanan Versi 5.0 dan pekeliling berkaitan seperti Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik Di Agensi-agensi Kerajaan.

Pentadbir e-mel berhak untuk membatalkan akaun **(pengguna yang berhenti, atau bertukar)** segera atas tujuan keselamatan maklumat.

Pentadbir e-mel boleh membekukan atau membuang akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus, tidak membuka akaun melebihi **180 hari bekerja (6 bulan)** atau pun menghadapi dikenakan tindakan tatatertib.

Pentadbir e-mel 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*. Pentadbir e-mel juga berhak mengakses semua e-mel yang dihantar dan diterima melalui sistem e-mel Kementerian Pertahanan bagi tujuan pemeriksaan sekiranya berlaku *security compromise*, aktiviti yang menyalahi undang-undang serta salah tingkah laku dalam penggunaan e-mel.

Bagi pengguna yang menggunakan peralatan mudah alih seperti telefon pintar, tablet, komputer peribadi dan sebagainya untuk mengakses e-mel, peralatan tersebut hendaklah dipastikan mematuhi langkah-langkah keselamatan sebagaimana yang telah ditetapkan di dalam DKICT.

Berikut adalah kaedah penggunaan akaun e-mel Kementerian Pertahanan:

i. **Pemilikan Akaun E-mel**

Pemilikan akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan kementerian dan boleh ditarik balik jika penggunaannya melanggar peraturan. Akaun atau alamat e-mel yang diperuntukkan oleh kementerian sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.

ii. Penghantaran

Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. Penghantar boleh menggunakan kemudahan 'salinan kepada' (Cc) sekiranya e-mel tersebut perlu dimaklumkan kepada penerima lain. Bagaimanapun, penggunaan '*blind cc*' (Bcc) tidak digalakkan.

Kemudahan '*reply*' digunakan untuk menjawab e-mel kepada penghantar asal dan '*forward*' untuk memanjangkan e-mel atau dimajukan kepada penerima lain. Kemudahan penghantaran e-mel jawab automatik semasa berada di luar pejabat bagi tempoh waktu yang panjang, boleh dipertimbangkan penggunaannya.

iii. 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. Perisian *Desktop Productivity* yang sering digunakan seperti *Microsoft Office* dan *Adobe Acrobat* mempunyai fungsi "*built-in*" enkripsi masing-masing. Bagi pengguna *Microsoft Office*, panduan penggunaan enkripsi perisian tersebut adalah seperti di **Lampiran A**, manakala bagi dokumen *PDF*, panduan adalah seperti di **Lampiran B**.

Bagi memperketatkan lagi keselamatan, pengguna dinasihatkan supaya memaklumkan katalaluan melalui medium yang berasingan misalnya perkhidmatan mesej segera seperti *Telegram*, *Signal* atau *WhatsApp*.

iv. Fail Kepilan (*Attachment*)

Saiz maksimum e-mel (termasuk kepilkan) samada untuk dihantar atau diterima adalah 10 MB. Jika saiz e-mel adalah agak besar, pengguna disarankan supaya menggunakan kaedah pemampatan (*compression*) bagi mengurangkan saiz fail (Contohnya menggunakan perisian *7zip*) Rujuk **Lampiran C**: Panduan Enkripsi Menerusi Program Pemampatan.

v. **Pengimbasan Fail Kepilan**

Pengguna hendaklah sentiasa mengimbas fail yang diterima sebelum membukanya. Pengguna juga hendaklah memastikan fail yang akan dihantar melalui e-mel adalah bebas dari virus.

vi. **Kenal Pasti Identiti Pengguna**

Setiap pengguna perlu mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan komunikasi dan transaksi maklumat melalui e-mel. Ini bertujuan untuk melindungi maklumat Kerajaan daripada sebarang bentuk penyalahgunaan.

vii. **Penerimaan Emel Tanpa Diminta (*Unsolicited E-mail*)**

Pengguna seharusnya mengelakkan dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. Ini bagi melindungi pengguna serta aset ICT kementerian Pertahanan daripada aktiviti yang tidak diingini seperti *phishing*, ancaman *virus*, *spamming* dan lain-lain *malware*.

viii. **Pengesanan Virus**

Pentadbir e-mel hendaklah dimaklumi segera sekiranya disyaki ada serangan virus dimana pengguna menerima mesej dari sistem mengenai *bounced mail* yang pengguna sendiri tidak hantar.

ix. **Penyimpanan**

Pengguna hendaklah memastikan jumlah e-mel yang disimpan di dalam kotak masuk e-mel (Inbox) adalah tidak melebihi ruang storan yang telah diperuntukkan dan mengutamakan penyimpanan e-mel yang perlu sahaja. Penyimpanan salinan e-mel pada sumber storan kedua seperti *hard disk* adalah digalakkan bagi tujuan keselamatan.

x. **Penghapusan dan Pemusnahan**

E-mel yang tidak penting dan tidak mempunyai nilai arkib atau e-mel yang telah diambil tindakan dan tidak diperlukan lagi bolehlah

dihapuskan. (Contoh: draf kertas kerja, draf minit, kertas makluman dan brosur). Emel yang berada di dalam *Folder Deleted Item* akan dimusnahkan secara kekal selepas 30 hari secara automatik.

Setiap pengguna adalah **DILARANG** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel ini seperti:

- i. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;
 - ii. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;
 - iii. Menggunakan e-mel untuk tujuan komersial, sosial atau politik;
 - iv. Menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;
 - v. Menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, e-mel sampah, e-mel *spam*, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Malaysia;
 - vi. Menyebarkan kod perosak seperti virus, *worm*, *trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;
 - vii. Menghantar e-mel sampah (*junk mail*) dan e-mel *spam*; dan
 - viii. Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.
 - ix. Semua pengguna e-mel perlu **memastikan** beberapa perkara berikut:
-

- x. memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan atau menerima sebarang e-mel yang meragukan;
- xi. bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel di dalam akaun sendiri dan tidak memberitahu kata laluan kepada pihak lain;
- xii. memaklumkan dengan kadar segera sekiranya peralatan mudah alih hilang atau dicuri;
- xiii. proses permohonan emel akan mengambil masa 3 hari bekerja dari tarikh borang permohonan diterima oleh Pentadbir e-mel; dan
- xiv. sekiranya e-mel tidak dibuka atau digunakan selama **6 bulan**, akaun e-mel tersebut akan dibuang dan tidak boleh digunakan lagi. Pemohon perlu membuat permohonan semula kepada Pentadbir e-mel.

6. PENGURUSAN REKOD-REKOD E-MEL

Rekod elektronik rasmi adalah merupakan rekod awam mengikut tafsiran Garis Panduan Pengurusan Rekod Elektronik yang diterbitkan oleh Arkib Negara Malaysia. Ia merangkumi sebarang mesej atau rekod komputer (termasuk fail keipilan) yang diwujudkan, dihantar, diserahkan, 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.

i. **Penyimpanan Rekod-Rekod E-mel**

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

menyimpan e-mel. Ini akan memudahkan carian dan mendapatkan kembali sesuatu e-mel.

ii. **Mencetak dan Memfail Rekod E-mel**

Rekod e-mel berkaitan sesuatu keputusan penting atau tindakan yang telah diambil hendaklah dicetak dan difailkan juga.

iii. **Penghapusan Rekod E-mel**

Pengguna hendaklah menghapuskan sebarang e-mel yang berunsurkan e-mel *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 juga boleh dihapuskan.

iv. **Backup Rekod E-mel**

Rekod e-mel penting yang telah berusia melebihi dua (2) bulan dan berkemungkinan besar akan dirujuk semula haruslah di *backup* (*export folder*) menggunakan *Microsoft Outlook Personal Folders Backup* iaitu semua data akan disimpan pada *Personal Folders file (.pst)* samaada dalam storan komputer peribadi (PC) atau luaran seperti *pen drive* atau cakera padat (CD). Ini akan mengurangkan penggunaan *mailbox* disamping membuat *backup* sebagai langkah keselamatan. (Rujuk **Lampiran D: Prosedur Pengurusan Archiving E-Mel**)

7. PENGURUSAN KATA LALUAN E-MEL

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Kementerian Pertahanan seperti berikut:

- i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
 - ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;
-

- iii. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf besar, huruf kecil, nombor dan aksara khusus. Contoh kata laluan yang kukuh: YfF@21Ca;
 - iv. Kata laluan hendaklah diingat dan **tidak boleh** dipaparkan atau didedahkan dengan apa cara sekalipun;
 - v. Kata laluan sistem pengoperasian dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;
 - vi. Kata laluan hendaklah ditukar semasa login kali pertama atau selepas kata laluan baharu diset semula;
 - vii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna, **tidak boleh** melibatkan nama pengguna sendiri dan mudah dijangka;
 - viii. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan
 - ix. Mengelakkan penggunaan semula kata laluan yang baru digunakan. Kata laluan yang sama **tidak boleh** diulang semula.
-

8. PROSES PERMOHONAN E-MEL

Langkah 1 – Permohonan oleh Pegawai/Kakitangan

- i. Pegawai/Kakitangan dikehendaki memuat turun borang permohonan e-mel di Portal Rasmi Kementerian Pertahanan (www.mod.gov.my) di pautan link borang (<http://www.mod.gov.my/index.php/ms/borang>);
- ii. Pegawai/Kakitangan perlu melengkapkan maklumat pengguna di borang tersebut;
- iii. Borang yang telah siap diisi perlu ditandatangani oleh Ketua Jabatan / Ketua Markas sebagai pengesahan; dan
- iv. Borang yang telah lengkap ditandatangani hendaklah dihantar ke Bahagian Pengurusan Maklumat (BPM) untuk tindakan selanjutnya.
- v. Bagi pengguna awam, boleh buat permohonan secara atas talian di pautan <https://sso.mod.gov.my/mohonemail/permohonanemail.php>

Langkah 2 – Semakan Permohonan

- i. BPM akan menyemak permohonan. Pihak BPM akan meluluskan permohonan yang telah lengkap.
- ii. Permohonan yang tidak lengkap akan dimaklumkan dan pemohon perlu melengkapkan maklumat yang berkaitan.

Langkah 3 – Mencipta e-mel Rasmi

- i. Pentadbir e-mel akan memproses Borang Permohonan E-mel yang lengkap dan mewujudkan akaun e-mel dalam tempoh satu (1) hari bekerja.
-

- ii. Pentadbir e-mel akan mencipta alamat e-mel pengguna berdasarkan kesesuaian permohonan.
- iii. Setiap pengguna diberikan mengikut kapasiti storan *mailbox* yang ditentukan oleh Kementerian.
- iv. Kapasiti storan *mailbox* pengguna akan diberikan tambahan (sekiranya perlu) seperti berikut:

Awam	
Gred ≤ 40	512 MB
Gred 41 – 44	1 GB
Gred 48 – 53	2 GB
Gred ≥ 54	5 GB
Perkhidmatan	
LLP (Pbt – PW I dan setaraf)	512 MB
Pegawai (Peg Kdt – Kapt dan setaraf)	1 GB
Pegawai (Mej – Kol dan setaraf)	2 GB
Pegawai Kanan (Brig Jen ke atas dan setaraf)	5 GB

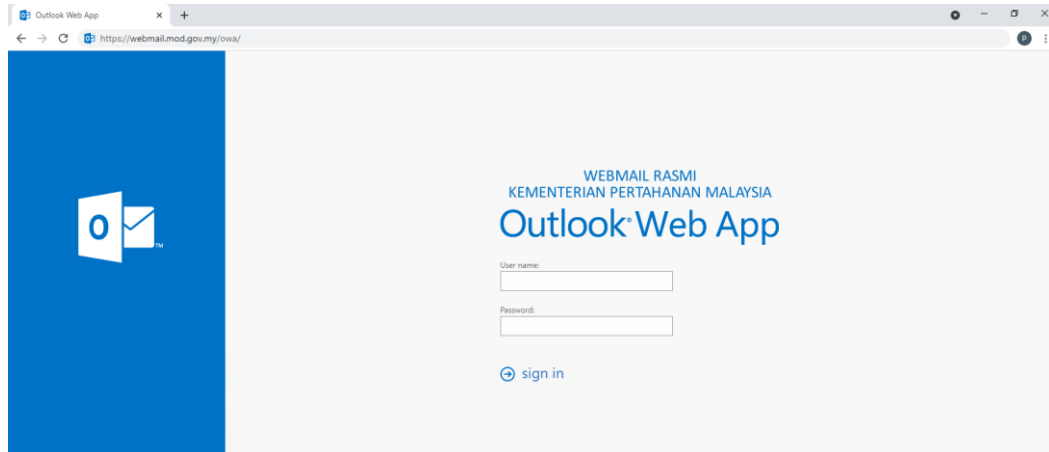
Jadual 1: Kuota Kapasiti Storán *Mailbox* E-Mel Kementerian Pertahanan

Langkah 4 – Pemberitahuan E-mel Diwujudkan

Pentadbir e-mel akan memaklumkan kelulusan kepada pemohon berkenaan melalui e-mel penyelia atau medium lain yang bersesuaian. Pengguna baru mesti menukar kata laluan sementara yang diberikan.

9. PENGGUNAAN PERTAMA KALI

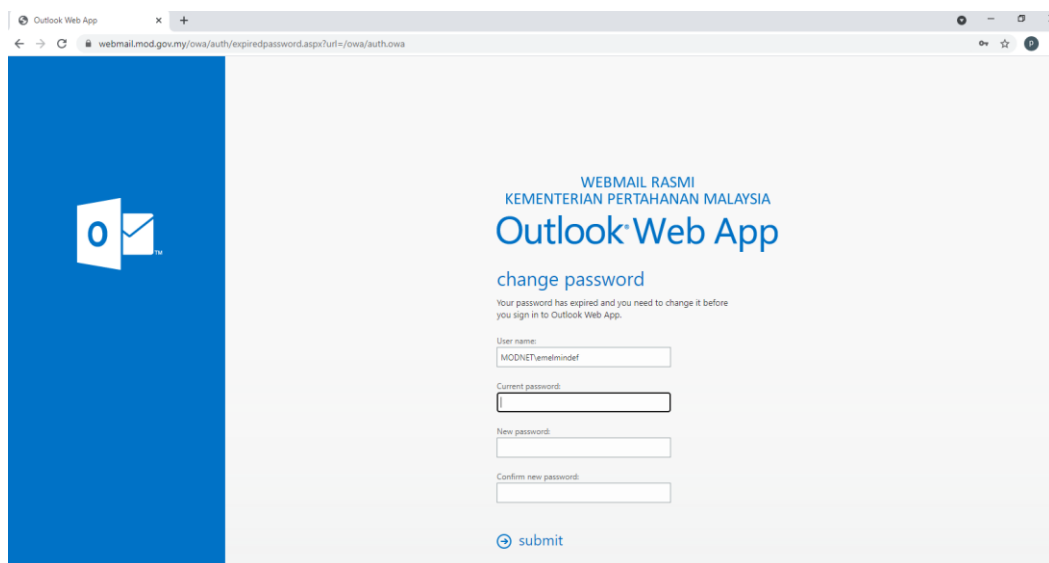
E-mel Kementerian juga boleh diakses melalui pautan *webmail* Kementerian Pertahanan di URL <https://webmail.mod.gov.my>.



Rajah 1: Paparan Antaramuka *Webmail* Kementerian Pertahanan

Pengguna perlu memasukkan *login ID* (sama ada nama atau nombor kad pengenalan) sahaja pada ruang *User name*.

Bagi penggunaan kata laluan pula, pengguna akan diminta untuk menukar kata laluan bagi setiap kali kata laluan baru diberikan.



Rajah 2: Paparan Antaramuka Penukaran Kata Laluan

10. TANGGUNGJAWAB PENGGUNA

Peraturan penggunaan dan pengurusan e-mel Kementerian Pertahanan ini adalah merupakan peraturan yang menggariskan tatacara penggunaan dan pengurusan rekod-rekod e-mel Kementerian Pertahanan. Semua pengguna e-mel Kementerian Pertahanan hendaklah mematuhi garis panduan ini.

11. MEJA BANTUAN

Sekiranya pegawai Kementerian Pertahanan mempunyai sebarang pertanyaan atau masalah, sila kemukakan kepada:

Help Desk BPM

Pentadbir E-mel

Bahagian Pengurusan Maklumat (BPM)

Kementerian Pertahanan

Tingkat 1, Wisma Pertahanan

Jalan Padang Tembak

50634 Kuala Lumpur

WhatsApp: 012-3524616 / 012-3143743

E-mel: pentadbiremel@mod.gov.my

Aduan secara *online* (eAduan ICT): <https://eaduanict.mod.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. Arahan Keselamatan (Semakan dan Pindaan 2017).
 9. Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT) Versi 5.0 – Kementerian Pertahanan, 2017.
-

GLOSARI

Warga MINDEF Kementerian Pertahanan	Semua kakitangan Kementerian Pertahanan Malaysia
Pengguna	Semua warga Kementerian Pertahanan yang menggunakan perkhidmatan e-mel mod.gov.my
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 Kementerian Pertahanan 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 Kementerian Pertahanan. Ianya tidak mempunyai kaitan langsung dengan tugas-tugas rasmi yang dijalankan oleh pegawai dan kakitangan Kementerian Pertahanan Malaysia.

<i>Mailbox</i>	Peti e-mel 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, diserahkan, 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 manamana perusahaan Kerajaan dan juga termasuk segala rekod yang, pada permulaan kuat kuasa Akta ini, adalah dalam jagaan atau di bawah kawalan Arkib Negara Malaysia.
------------	--

LAMPIRAN A

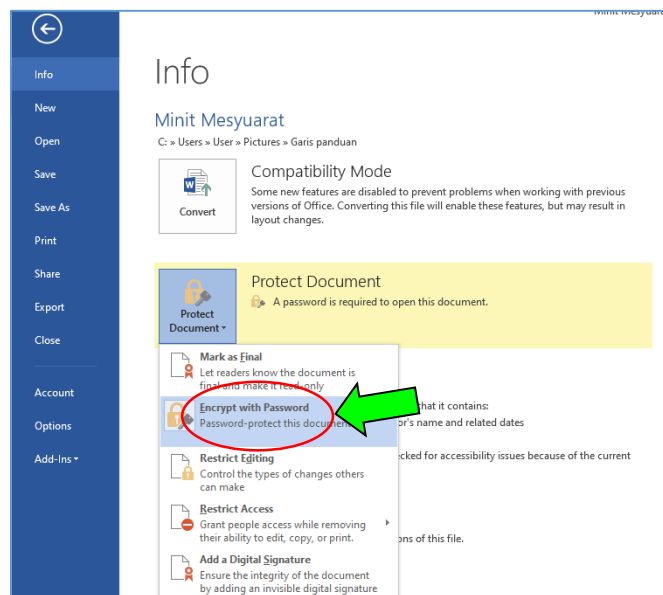
PANDUAN ENKRIPSI / DEKRIPSI MICROSOFT OFFICE 2013

PENGENALAN

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

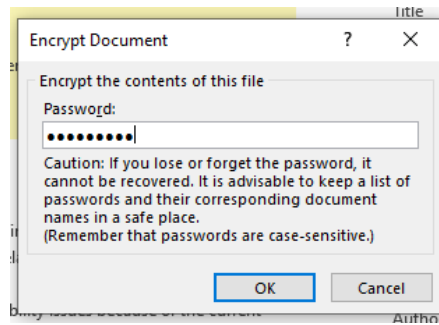
LANGKAH-LANGKAH

1. Buka dokumen (.docx, .xlsx, .pptx) yang hendak dienkrp. Contoh yang ditunjukkan adalah Microsoft Word 2013.
2. Buka fail dan pilih **File > Info > Protect Document > Encrypt with Password** seperti Rajah 1.



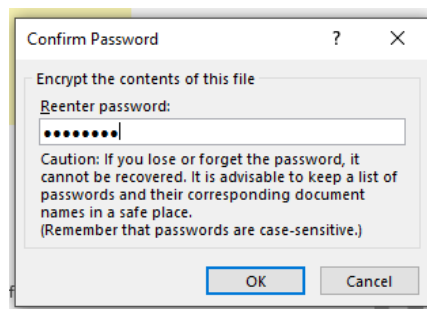
Rajah 1: Kaedah enkripsi dokumen dalam Microsoft Word

3. Sila masukkan kata laluan yang difikirkan sesuai dan kukuh yang mematuhi Dasar Keselamatan ICT Kementerian Pertahanan pada kotak kemasukan kata laluan (Rajah 2) dan klik **OK** setelah selesai.



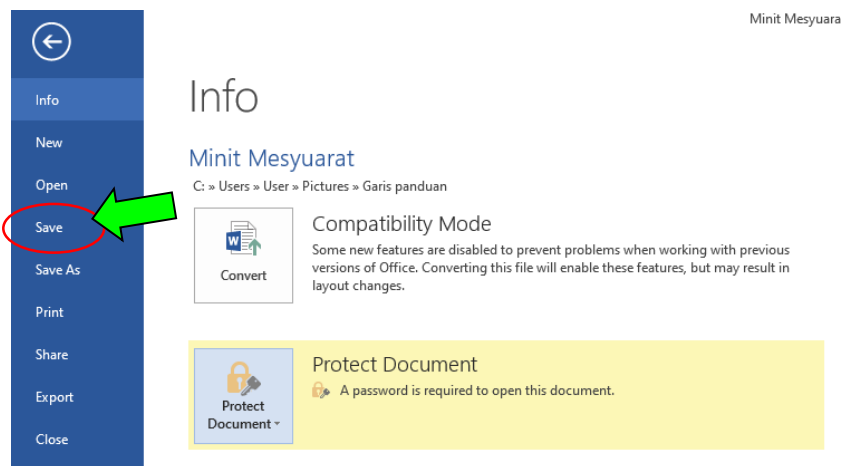
Rajah 2: Penetapan kata laluan untuk mengenkrip dokumen

4. Masukkan kata laluan yang sama pada skrin pengesahan kata laluan yang dipaparkan dan klik **OK** setelah selesai.



Rajah 3: Pengesahan kata laluan yang telah dimasukkan

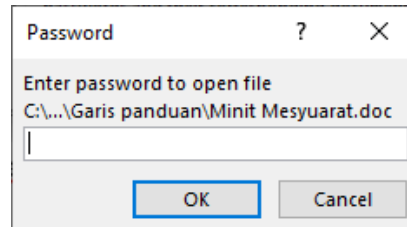
5. Sila klik pilihan **Save** setelah selesai. Ini bagi memastikan penetapan kata laluan dilaksanakan dengan sempurna.



Rajah 4: Dokumen telah dilindungi kata laluan selepas butang **Save** diklik

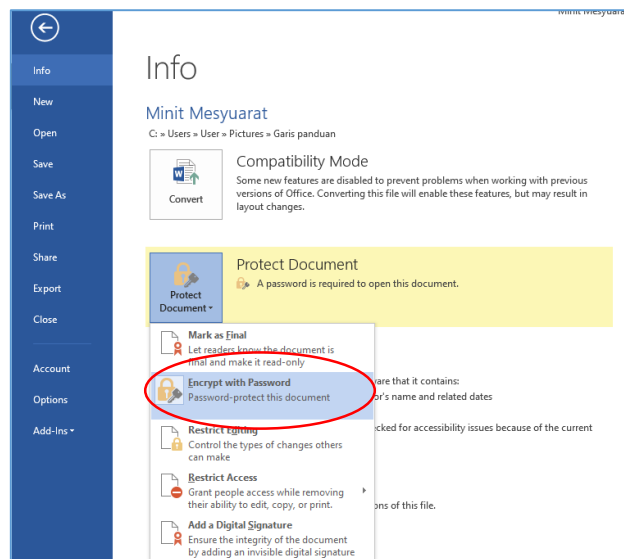
6. Dokumen tersebut kini boleh diedarkan secara elektronik.

7. Seterusnya, pemilik dokumen perlu memaklumkan penerima tentang kata laluan melalui saluran komunikasi lain seperti panggilan telefon atau mesej Telegram, Signal, WhatsApp untuk membuka dokumen berkenaan.
8. Dokumen tersebut kini memerlukan kata laluan sebelum boleh dibuka dan/atau diubahsuai oleh penerima (rujuk Rajah 5).



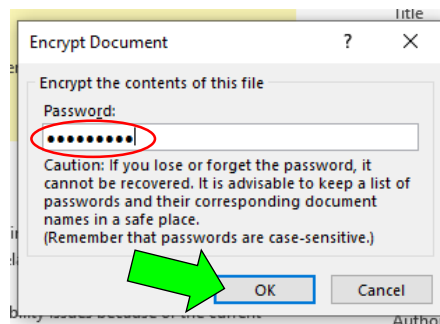
Rajah 5: Kotak dialog kata laluan untuk buka dokumen yang telah dienkrip

9. Untuk membatalkan enkripsi, sila pilih **File > Info > Protect Document > Encrypt with Password** (rujuk Rajah 6).



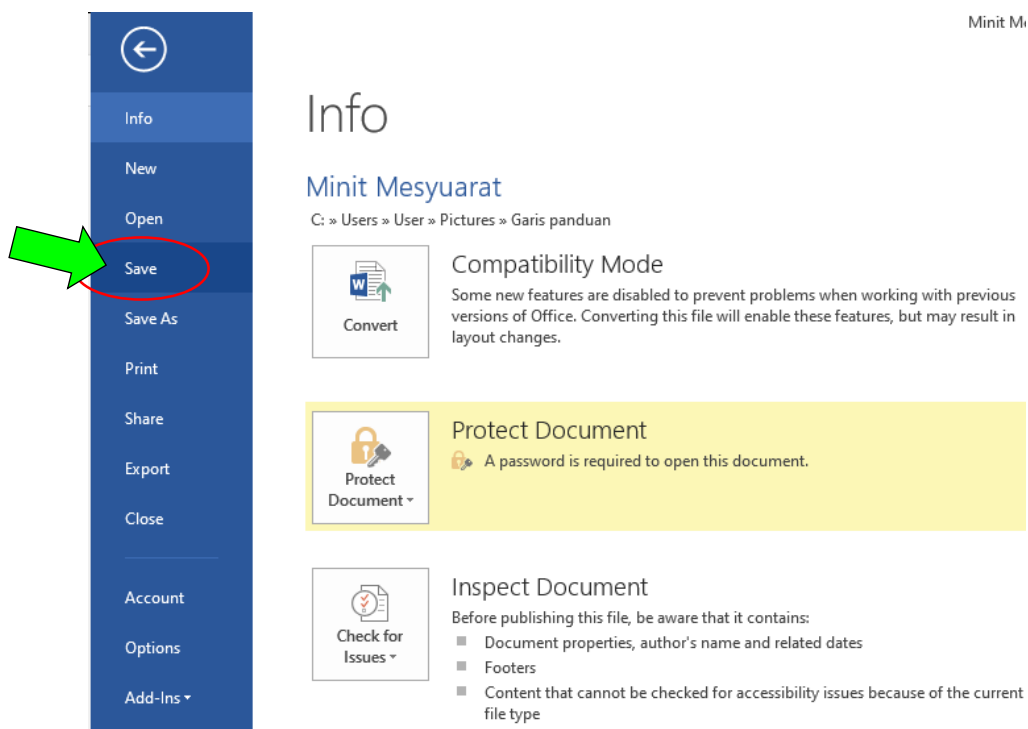
Rajah 6: Pembatalan enkripsi yang telah dilaksanakan

10. Padamkan (**delete**) kata laluan yang telah dimasukkan (kata laluan dipaparkan sebagai simbol titik), kemudian klik **OK** seperti Rajah 7.



Rajah 7: Pemadaman kata laluan yang telah ditetapkan

11. Sila klik pilihan **Save** setelah selesai. Ini bagi memastikan perubahan yang dilaksanakan dapat disimpan.



Rajah 8: Dokumen telah diubah selepas butang **OK** diklik

LAMPIRAN B

PROSEDUR ENKRIPSI DOKUMEN FORMAT PDF

PENGENALAN

Bahagian ini akan menerangkan prosedur enkripsi yang boleh dilakukan ke atas dokumen berformat PDF sebagai langkah keselamatan asas. Program yang digunakan dalam tutorial ini ialah **PDFEncrypt**, satu program *open source* yang selamat dan boleh dimuat turun dari <https://pdfencrypt.net/files/setup.exe>.

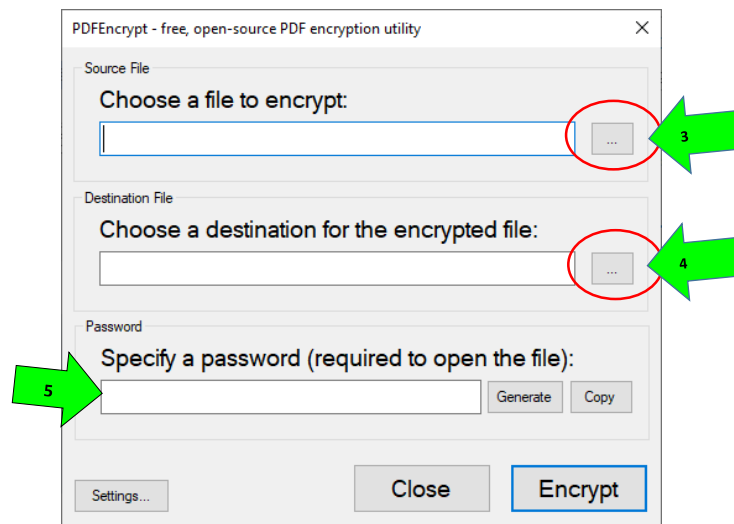
LANGKAH-LANGKAH

1. Muat turun dan install **PDFEncrypt** terlebih dahulu.
2. Selepas selesai instalasi, **dwi-klik** ikon **PDFEncrypt** (Rajah 1) pada paparan Desktop.



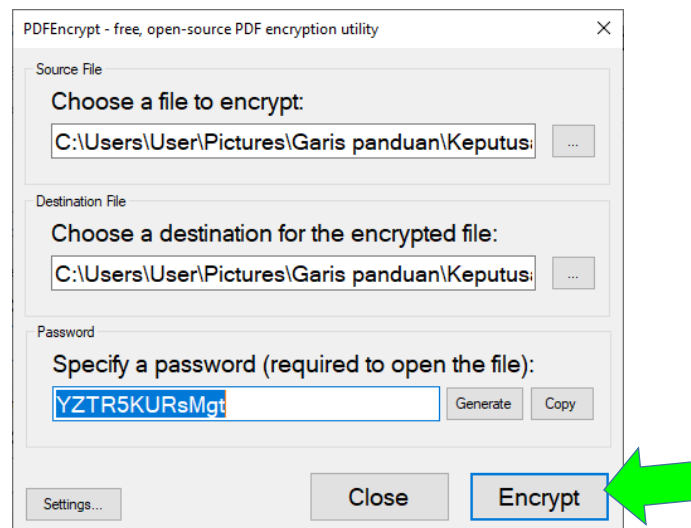
Rajah 1: Ikon PDF Encrypt

3. Paparan kekotak dialog berikut (Rajah 2) akan terbuka. Sila klik butang titik-titik di hujung kotak teks "*Choose a file to encrypt*" untuk pilih dokumen PDF yang hendak dienkrip.
-



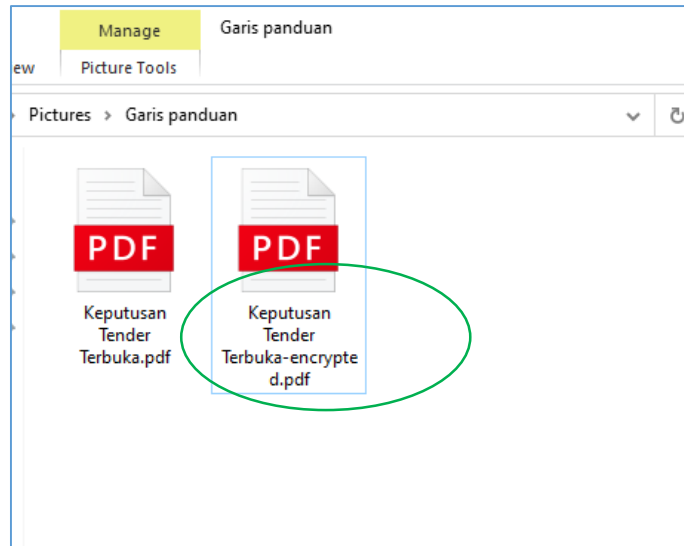
Rajah 2: Kotak dialog

4. Pada kotak dialog yang sama, klik butang titik-titik di hujung “*Choose a destination ...*” dan pilih lokasi untuk menempatkan fail PDF yang telah diencrip kelak.
5. Kemudian, taip kata laluan (*password*) untuk fail PDF tersebut. Anda juga boleh menggunakan *password* rawak dengan menekan butang “*Generate*” di hujung kotak teks “*Specify a password ...*”(Rajah 3). Pastikan *password* tersebut disalin agar tidak lupa. Kemudian, klik butang “*Encrypt*”.



Rajah 3: Kotak dialog

- Dokumen PDF yang telah selesai dienkrip akan muncul dalam folder destinasi. Dokumen yang telah dienkrip ditandai dengan tambahan nama “-encrypted.pdf” di hujung nama dokumen yang asal seperti ditunjukkan dalam Rajah 4.



Rajah 4: Fail PDF telah selesai dienkrip

- Dokumen PDF ini sedia dikepilkan sebagai lampiran dalam e-mel rasmi dan dihantar kepada bakal penerimanya manakala kata laluannya perlu dikiriskan menerusi saluran berbeza seperti Telegram, Signal atau WhatsApp.

LAMPIRAN C

PROSEDUR ENKRIPSI MENERUSI PROGRAM PEMAMPATAN

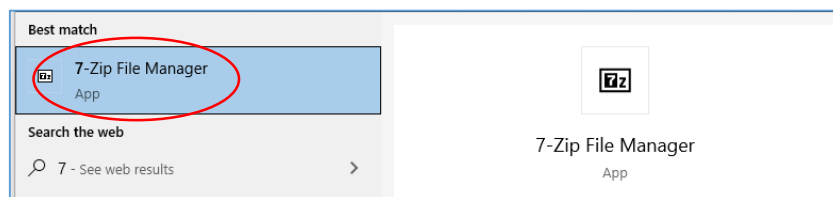
PENGENALAN

Apabila perlu menghantar sebilangan fail dalam lampiran e-mel, cara paling praktikal ialah dengan menyatukan fail-fail tersebut dalam satu fail yang termampat. Bahagian ini akan menerangkan prosedur enkripsi / dekripsi yang boleh dilakukan atas fail mampatan berkaitan sebagai langkah keselamatan asas.

Program yang digunakan dalam tutorial ini ialah **7-Zip**, satu program *open source* yang selamat dan boleh dimuat turun dari <https://www.7-zip.org/a/7z1900-x64.exe>.

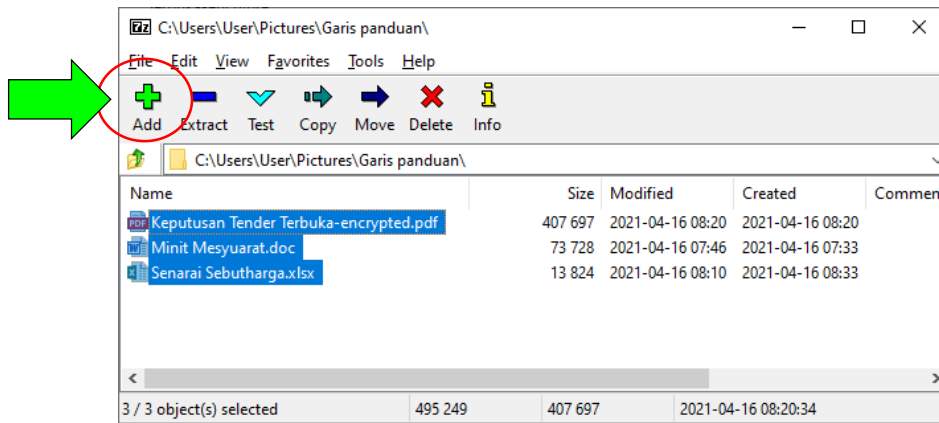
LANGKAH-LANGKAH

1. Muat turun dan install program **7-Zip** terlebih dahulu.
2. Selepas selesai instalasi, klik ikon **7-Zip File Manager** (Rajah 1) daripada pilihan menu start.



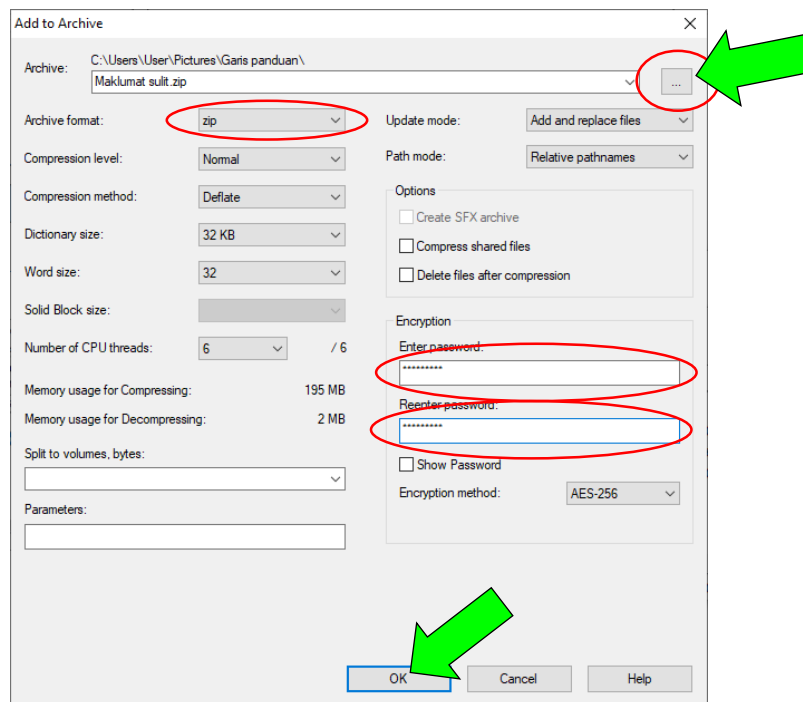
Rajah 1: Ikon 7zip pada menu start

3. Apabila kotak dialog (Rajah 2) muncul, tekan (jangan lepas) butang **Ctrl** (pada *keyboard*) dan klik pada dokumen-dokumen yang hendak dimampatkan bersama, diikuti klik pada ikon "**Add**".
-



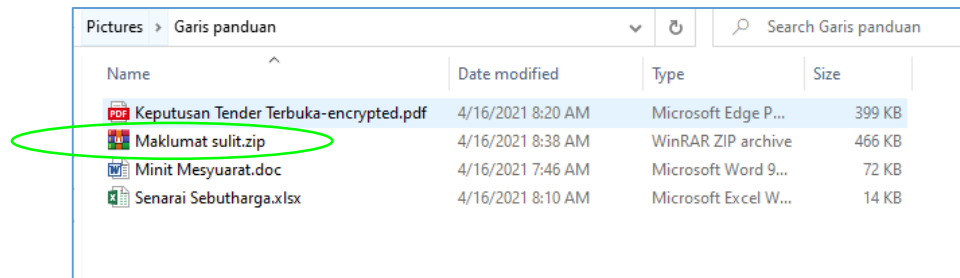
Rajah 2: Kotak dialog pemilihan fail untuk dimampatkan

4. Kotak pada Rajah 3 akan muncul. Klik butang titik-titik di hujung kotak teks “**Archive:**” untuk menentukan destinasi output proses ini kelak.
5. Pada Rajah 3 juga, pilih format **zip** daripada senarai “**Archive Format:**”. Taipkan kata laluan pada ruangan **Encryption**. Anda perlu menaip dua kali kata laluan yang sama dalam ruangan tersebut. Kemudian klik OK.



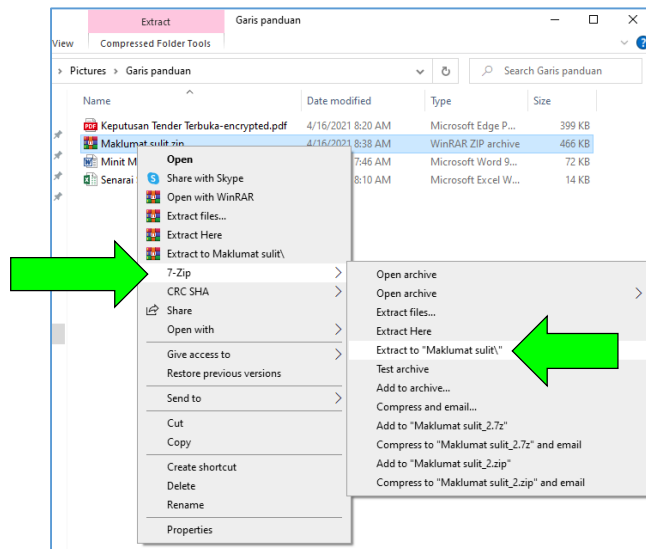
Rajah 3: Kotak dialog “Add to archive”

6. Fail termampat akan terhasil di lokasi destinasi seperti ditunjukkan dalam Rajah 4.



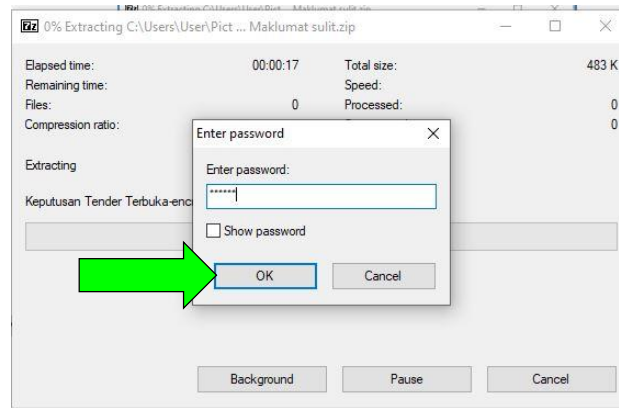
Rajah 4: Fail mampatan terhasil dalam format .zip

7. Bagi membuka fail mampatan tersebut, klik kanan pada fail zip itu dan pilih **7-Zip** > **Extract to** “.. seperti di Rajah 5.



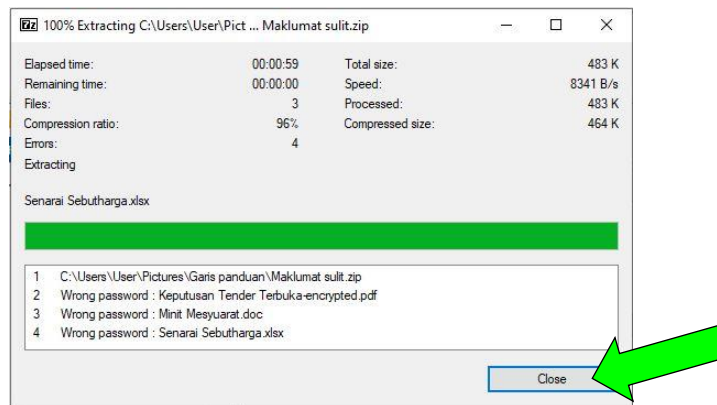
Rajah 5: Proses mengekstrak kandungan fail termampat

8. Kotak dialog seperti Rajah 6 akan muncul meminta kata laluan ditaip. Sila taip kata laluan untuk mula mengekstrak fail mampatan itu dan klik **OK**.



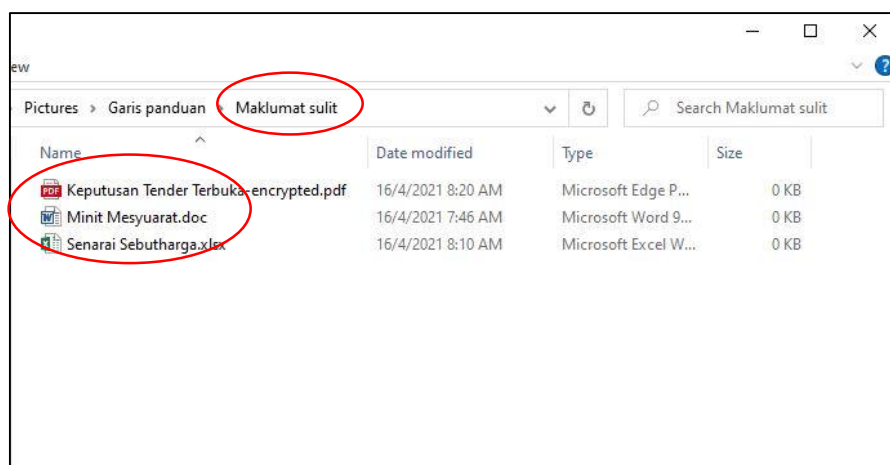
Rajah 6: Kotak dialog untuk input kata laluan bagi membuka fail zip

9. Kata laluan yang betul akan memaparkan Rajah 7 seperti di bawah. Klik butang **Close**.



Rajah 7: Kotak dialog progress

10. Hasil pengekstrakan akan muncul dalam folder dengan nama yang sama dengan fail zip tadi.



Rajah 8: Paparan dokumen setelah diekstrak

LAMPIRAN D

PROSEDUR PENGARKIBAN E-MEL

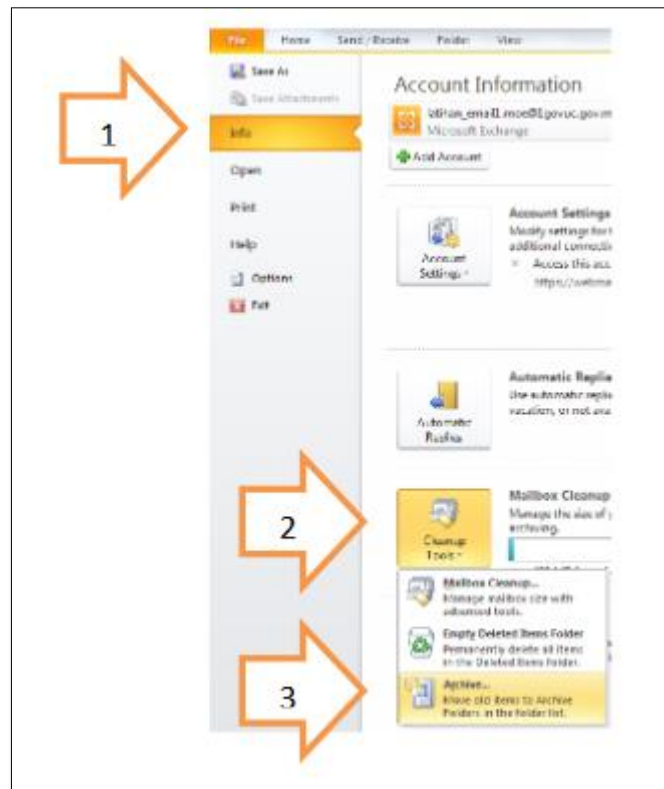
PENGENALAN

Kemudahan pengarkiban e-mel hanya boleh dilaksanakan Microsoft Outlook sahaja. Sekiranya saiz kapasiti storan *mailbox* telah penuh, cara yang paling praktikal adalah dengan memindahkan item lama ke fail simpanan secara manual dengan memilih Arkib pada menu Fail. Atau anda boleh memindahkan fail lama secara automatik dengan menggunakan ciri *AutoArchive*. Item dianggap lama ketika mencapai usia yang anda tentukan. Dengan ciri *AutoArchive*, anda boleh memadam atau memindahkan item lama. Bahagian ini akan menerangkan langkah-langkah bagi proses *archiving*.

Anda disarankan untuk membuat proses arkib sekiranya *mailbox* anda telah mencecah 80% penuh bagi mengelakkan sebarang permasalahan *inbox* penuh dan tidak menerima sebarang e-mel.

➤ LANGKAH-LANGKAH UNTUK MENCIPTA FAIL *ARCHIVE*

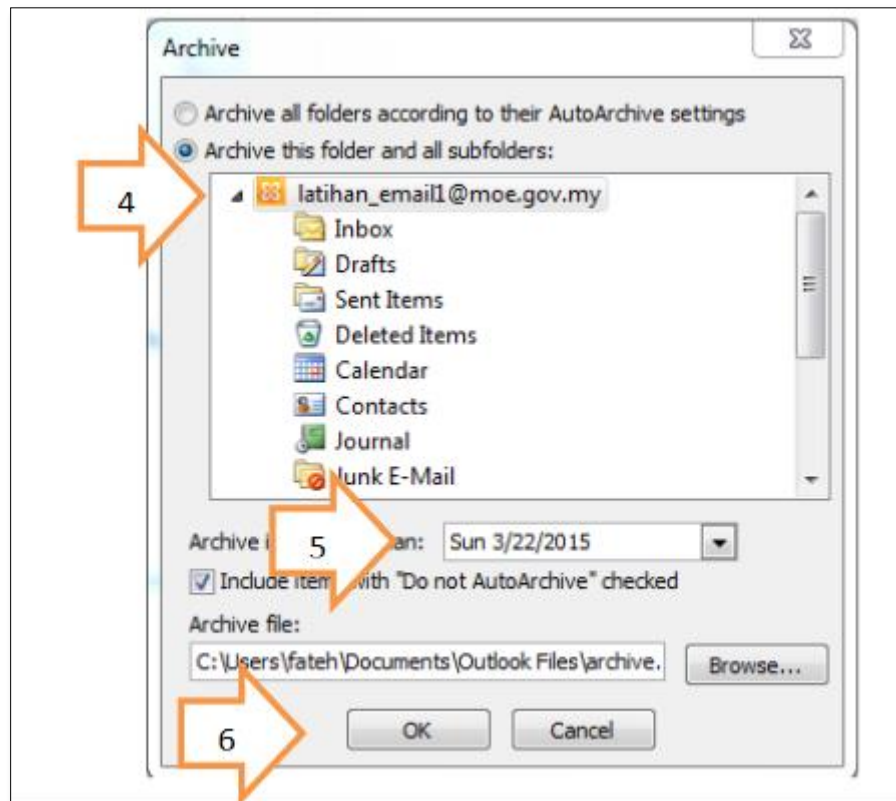
1. Pada menu bar, pilih **File** dan klik **Info**
 2. Klik Icon **Cleanup Tools**
 3. Pilih **Archive**
-



Rajah 1: Ikon Info pada menu File

4. Pada tettingkap Archive, klik pada **alamat e-mel anda**
5. Klik Icon Cleanup Tools Sila kenalpasti **tarikh e-mel** yang hendak di masukkan ke dalam folder *archive*.

Contoh: Tarikh yang dipilih menentukan tempoh e-mel yang ingin disimpan di dalam folder archive. Sekiranya tarikh yang dikenalpasti adalah 22/3/15, maka sistem akan menyimpan semua e-mel yang diterima sebelum 22/3/15 ke dalam folder archive.



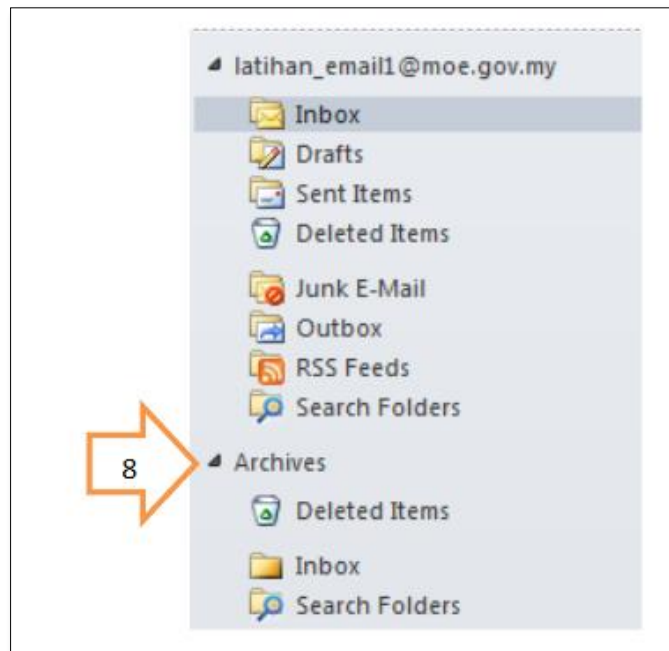
Rajah 2: Kotak dialog untuk pilihan *folder*, tarikh dan *archive file*

6. Klik **Ok**
7. Proses arkib akan dilaksanakan oleh Microsoft Outlook seperti di bawah.



Rajah 3: Kotak dialog proses pengarkiban

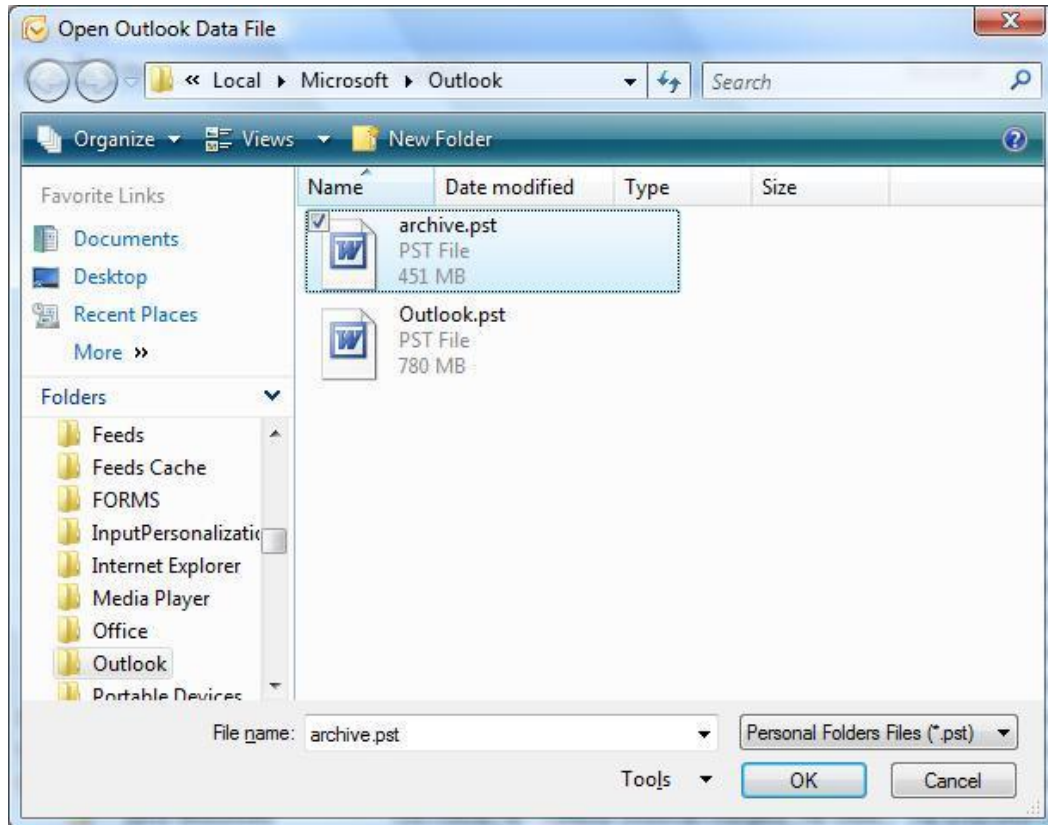
8. Setelah proses arkib selesai. Anda akan dapati e-mel yang telah diarkib akan dipaparkan pada *folder* arkib seperti di bawah.



Rajah 4: Paparan e-mel yang telah selesai arkib

➤ **LANGKAH-LANGKAH UNTUK MEMBUKA FAIL ARKIB**

1. Pada menu bar, pilih **File** dan klik **Open / Outlook Data File**.
2. Pilih fail **archive** untuk dibuka (*.pst)

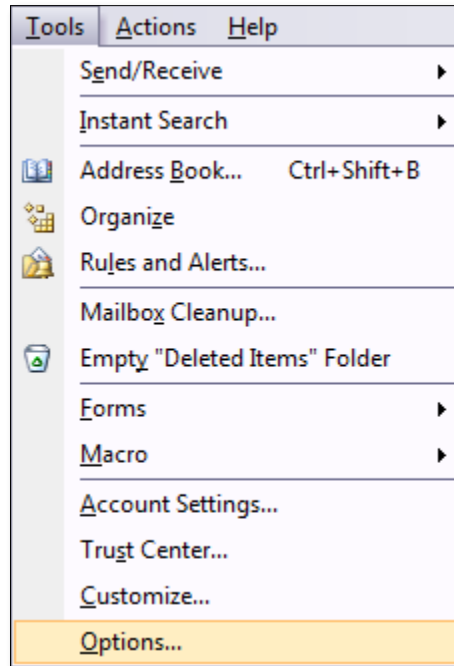


Rajah 1: Kotak untuk memilih file .pst

3. Klik **Ok**
4. Fail tersebut akan terpapar di ruang "**Mail Folders**"

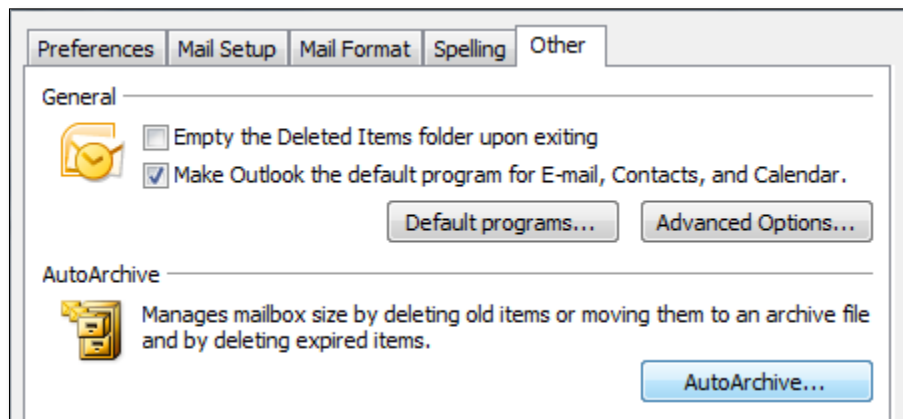
➤ LANGKAH-LANGKAH UNTUK KONFIGURASI *AUTOARCHIVE*

1. Pada menu bar, pilih **Tools** dan klik **Option**



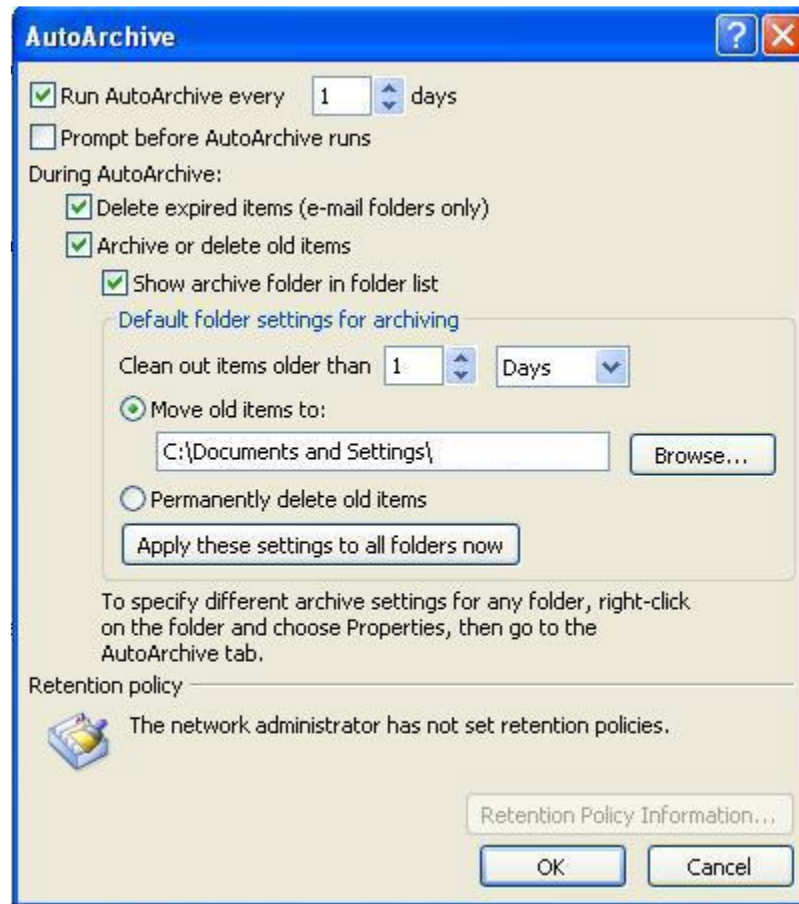
Rajah 1: Ikon *option* pada menu tools

2. Klik pada tab "**other**" dan butang **AutoArchive**



Rajah 2: Kotak dialog untuk pilih *tab 'Other'*

3. Sila tentukan pilihan mengikut kesesuaian pengguna:
 - i. Bilangan hari proses **autoarchive**
 - ii. **Kekerapan** untuk melakukan pembersihan atau perpindahan e-mel yang lama

Rajah 3: Kotak dialog *autoarchive*

4. Klik **Ok**.