PROSEDUR ENKRIPSI MAKLUMAT TERPERINGKAT

WINRAR

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 & Communicat ions Technology Security Handbook (MyMIS) Version 2.0*.

(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	Rahsiabesar	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 pelindungan 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 rangkaianlain.				Tidak diperlukan
Menghantar / Memindahkan					
Menghantar maklumat melalui Rangkaian Awam	Menggunakan kaedah enkripsi				Tidak diperlukan

Jadual 1: Pengendalian Maklumat Elektronik

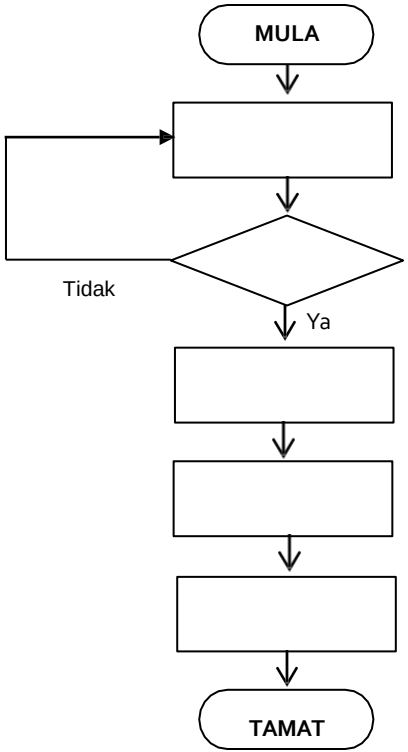
6.0 PROSES ENKRIPSI MAKLUMAT TERPERINGKAT

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 pengkelasan dan pelabelan maklumat rasmi mengikut pengelasannya 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

[7]

PROSEDUR ENKRIPSI WINRAR

JABATAN HAL EHWAL AGAMA TERENGGANU

PROSEDUR ENKRIPS IWINRAR

PENGENALAN

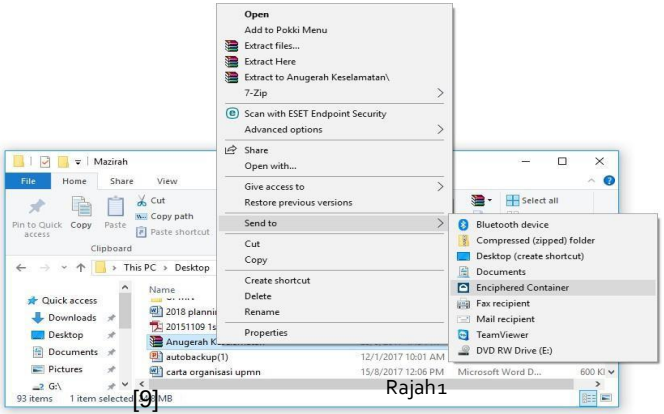
Aplikasi Winrar sering digunakan untuk mengecilkan saiz folder yang besar untuk memudahkan penghantaran melalui emel.

1. ***Download*** aplikasi encipher.it di https://encipher.it/download

2. ***Run*** aplikasi encipher.it pada komputer

3. Klik kanan dan ***Send to*** fail .zip ke ***Encipheres Container***

Nota: Sila Rujuk Rajah1



Rajah1

ENKRIPSI WINRAR

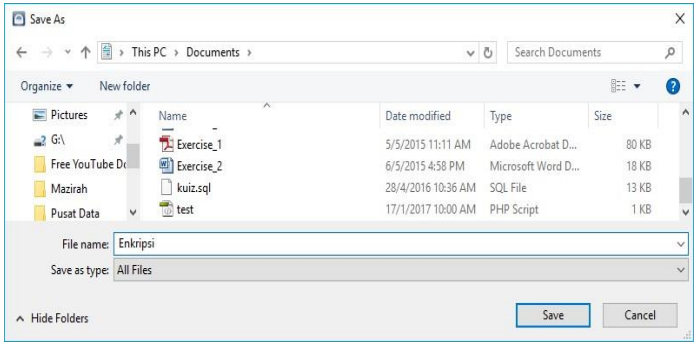
4. Masukkan ***password*** dan klik ***save to file***

   Nota: Sila Rujuk Rajah 2

Rajah 2

5. ***Save*** nama fail yang dikehendaki

   Nota: Sila Rujuk Rajah 3



Rajah 3

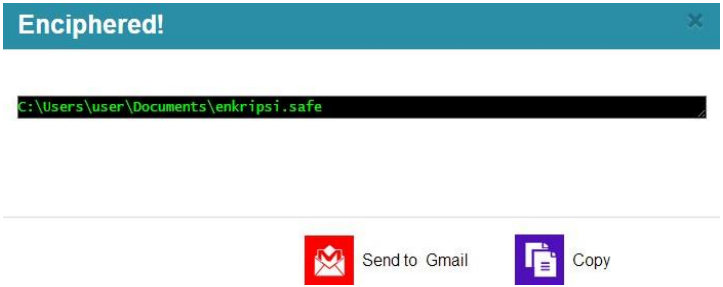
[10]

6. Enkripsi berjaya

7.Seterusnya pemunya fail winrar akan memaklumkan penerima tentang kata laluan melalui emel ataupun telefon bagi membuka fail winrar berkenaan

8. Fail winrar tersebut kini memerlukan kata laluan sebelum boleh dibuke dan/atau diubahsuai oleh penerima

Nota: Sila Rujuk Rajah4



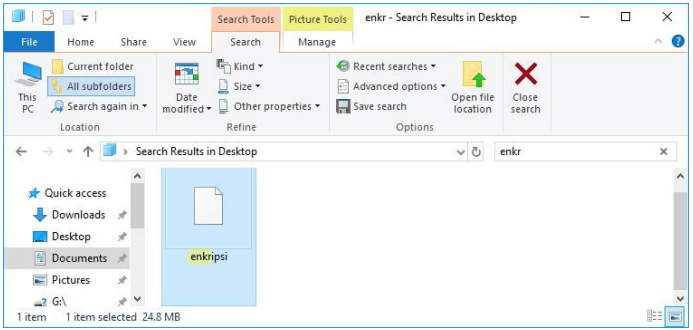
Rajah4

PROSEDUR DEKRIPSI WINRAR

DEKRIPSI WINRAR

1. ***Double click*** pada fail winrar yang telah dibuat enkripsi.

   Nota: Sila Rujuk Rajah1

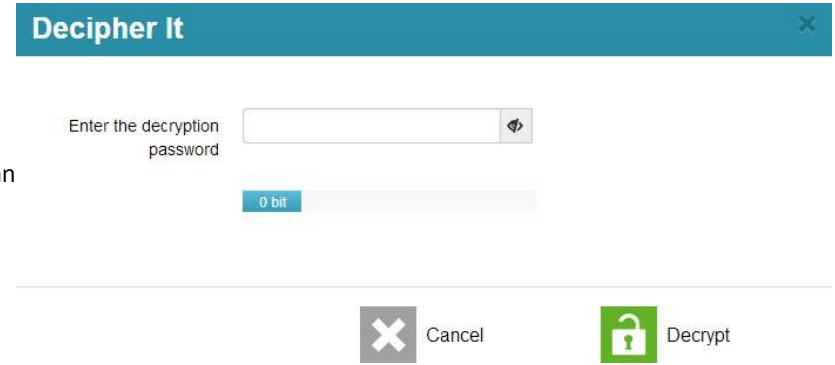


Rajah1

2. Masukkan password yang telah ditetapkan

3. Klik pada butang ***Decrypt***

   Nota: Sila Rujuk Rajah 2



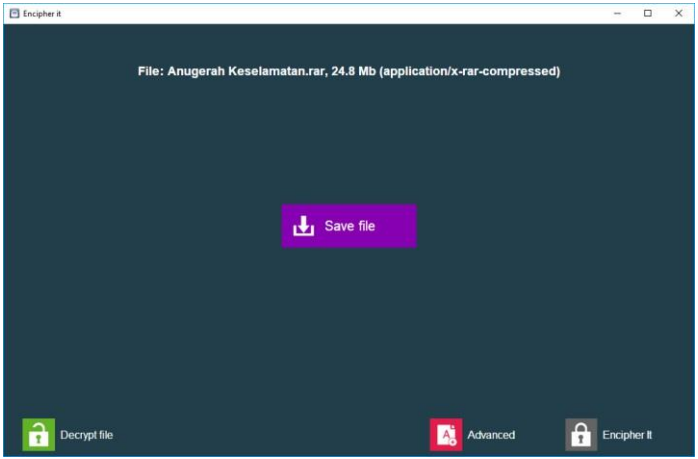
[12]

Rajah2

4. Proses dekripsi selesai

5. Save File winrar tersebut untuk di ***unzip***

Nota: Sila Rujuk Rajah3



Rajah3

DISEDIAKANOLEH:

UNIT TEKNOLOGI MAKLUMAT
JABATAN HAL EHWAL AGAMA TERENGGANU