



KETUA PENGARAH  
UNIT PEMODENAN TADBIRAN DAN PERANCANGAN  
PENGURUSAN MALAYSIA (MAMPU)  
JABATAN PERDANA MENTERI  
ARAS 6, BLOK B2  
KOMPLEKS JABATAN PERDANA MENTERI  
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN  
62502 PUTRAJAYA  
MALAYSIA



PENGIKTIRAFAN MS ISO 9001: 2000 NO. SIJIL: KLR 0500331

Telefon : 03-88882311  
Faks : 03-88883163  
Email : normah@mampu.gov.my

MAMPU.702-1/1/7 Jld. 3 (48)

23 Mac 2009

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua Ketua Badan Berkanun Persekutuan

Semua Y.B. Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Tempatan

Y.B./Y.Bhg. Tan Sri/Datuk/Dato'/Dr./Tuan/Puan,

**PENGAKTIFAN FAIL LOG SERVER BAGI TUJUAN  
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT  
DI AGENSI-AGENSI KERAJAAN**

Dengan hormatnya saya merujuk perkara di atas.

2. Sebagaimana Y.B./Y.Bhg. Tan Sri/Datuk/Dato'/Dr./Tuan/Puan sedia maklum, pasukan *Government Computer Emergency Response Team* (GCERT) telah ditubuhkan di MAMPU pada 2 Januari 2001 selaras dengan Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan (Pekeliling Am Bil. 3 Tahun 2000) bagi mengendalikan insiden keselamatan ICT Sektor Awam.

3. Sepanjang tahun 2008, sebanyak 153 insiden keselamatan ICT telah dilaporkan kepada GCERT. Namun begitu, terdapat **52 insiden keselamatan ICT (34 %) tidak dapat disiasat kerana fail log tidak diaktifkan.**

4. Sehubungan dengan itu, semua Ketua Jabatan adalah dipohon untuk memastikan fail log bagi server dan aplikasi di agensi tuan diaktifkan:

- i) Fail log sistem pengoperasian;
- ii) Fail log servis (cth: web, ftp, emel, dll.);
- iii) Fail log aplikasi (audit trail); dan
- iv) Fail log rangkaian (cth: switch, firewall, router, IDS/IPS, dll.).

5. Bagi agensi kerajaan yang menggunakan perkhidmatan *web hosting* bagi perkhidmatan laman web/portal dan emel agensi, sila pastikan fail log berasingan diaktifkan dengan merujuk panduan seperti di lampiran. Panduan ini juga terdapat di laman web GCERT, <http://gcert.mampu.gov.my>.

6. Fail log berkenaan hendaklah **disimpan untuk tempoh sekurang-kurangnya 6 bulan** di tempat yang selamat dan **dikemukakan kepada MAMPU apabila diperlukan** untuk pengurusan pengendalian insiden keselamatan ICT.

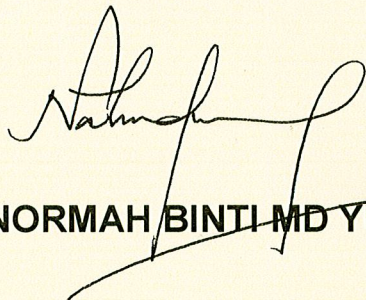
7. Maklumat lanjut mengenai pengendalian insiden keselamatan ICT boleh diperolehi dari **Pekeliling Am Bil. 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"**, **Pekeliling Am Bil. 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"** dan **Surat Pekeliling Am Bil. 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam"** yang boleh diperolehi dari laman web MAMPU, <http://www.mampu.gov.my>.

8. Semua Ketua Jabatan diminta mengambil tindakan di atas serta memastikan pekeliling-pekeliling berkaitan pengurusan pengendalian insiden keselamatan ICT dipatuhi, dilaksanakan dan dipantau.

Sekian, terima kasih.

**“BERKHIDMAT UNTUK NEGARA”**

Saya yang menurut perintah,



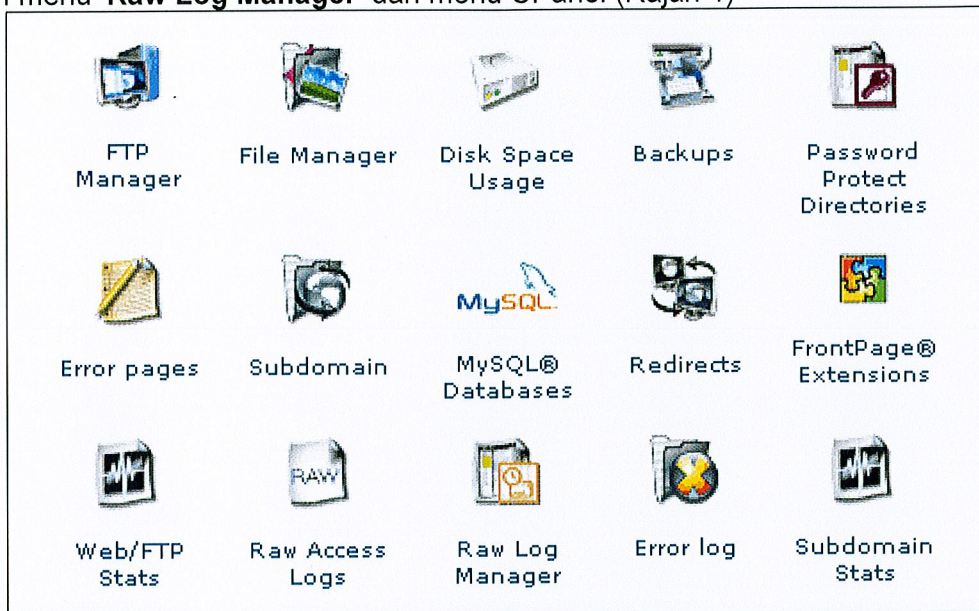
**(DATO' NORMAH BINTI MD YUSOF)**

s.k.

**Y.Bhg. Tan Sri Mohd Sidek bin Hassan**  
Ketua Setiausaha Negara  
Pejabat Ketua Setiausaha Negara  
Aras 4, Blok Timur  
Bangunan Perdana Putra  
Pusat Pentadbiran Kerajaan Persekutuan  
62502 PUTRAJAYA

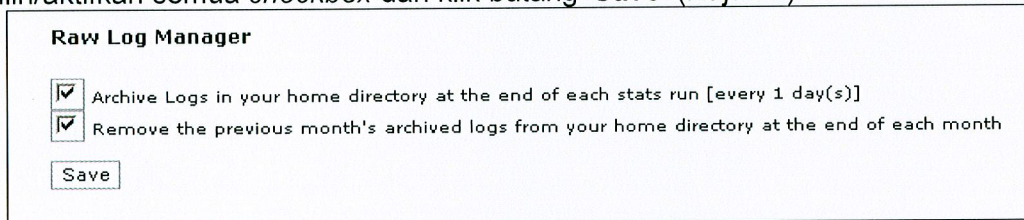
## PANDUAN MENGAKTIFKAN FAIL LOG MENGGUNAKAN CPANEL

1. Pilih menu **'Raw Log Manager'** dari menu CPanel (Rajah 1)



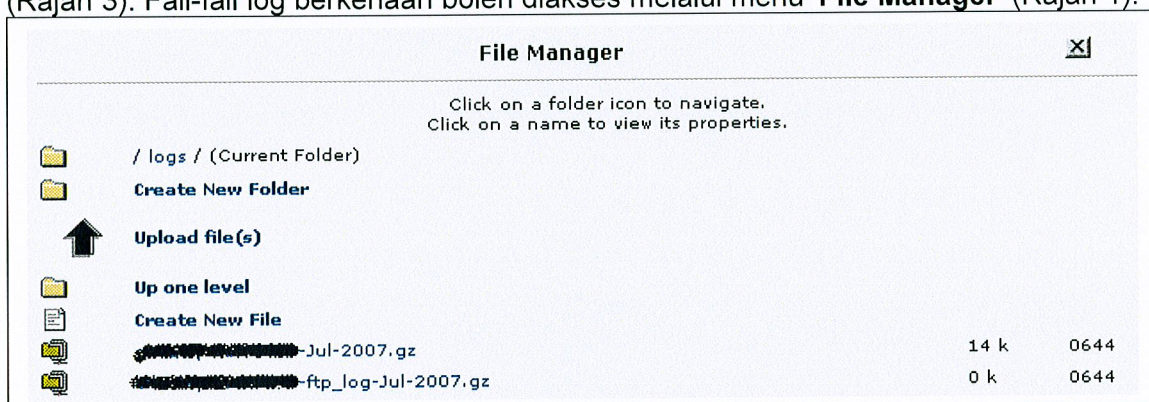
Rajah 1 : Menu CPanel

2. Pilih/aktifkan semua *checkbox* dan klik butang **'Save'** (Rajah 2).



Rajah 2 : Konfigurasi 'Raw Log Manager'

3. Semua fail-fail log bagi akaun *web hosting* berkenaan akan disimpan di folder **/logs** (Rajah 3). Fail-fail log berkenaan boleh diakses melalui menu **'File Manager'** (Rajah 1).



Rajah 3 : Senarai Fail Log