DASAR KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)
JABATAN PERANCANGAN BANDAR DAN DESA NEGERI SELANGOR

1. PENGENALAN

Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) ini yang dikeluarkan oleh Jawatankuasa Keselamatan ICT Jabatan, JPBD Selangor adalah berdasarkan kepada garis panduan dan pekeliling yang telah dikeluarkan oleh MAMPU. Pekeliling yang diguna pakai bagi keselamatan ICT sektor awam adalah Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi.

Keselamatan ICT berdasarkan pekelilng tersebut meliputi semua data, peralatan, perisian, rangkaian dan kemudahan ICT yang lain. Untuk memastikan maklumat dan data penting Jabatan bebas daripada sebarang ancaman, semua pengguna adalah disarankan untuk mematuhi garis panduan ini.

2. OBJEKTIF

Tujuan utama Dasar Keselamatan ICT JPBD Selangor adalah sebagai panduan untuk pengguna demi menjamin kesinambungan urusan Kerajaan dengan meminimumkan kesan insiden keselamatan. Keselamatan ICT berkait rapat dengan pelindungan maklumat dan aset ICT. Ini kerana komponen peralatan dan perisian yang merupakan sebahagian daripada aset ICT Kerajaan adalah pelaburan besar yang perlu dilindungi. Begitu juga dengan maklumat yang tersimpan di dalam system ICT. Ia amat berharga kerana banyak sumber yang telah digunakan untuk menghasilkannya dan sukar untuk dijana semula dalam jangkamasa yang singkat. Tambahan pula terdapat maklumat yang diproses oleh sistem ICT adalah sensitif dan terperingkat. Pendedahan tanpa kebenaran atau pembocoran rahsia boleh memudaratkan kepentingan negara. Sebarang penggunaan aset ICT kerajaan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Kerajaan.

Justeru, dasar ini diwujudkan supaya menjadi panduan kepada para pengguna agar kesahihan, keutuhan dan kebolehsediaan maklumat yang berterusan sentiasa terjamin.

3. KESELAMATAN ICT

Keselamatan merupakan proses yang berterusan dan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Ia meliputi:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses kepada hanya pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas. Dasar ini diharapkan dapat menjamin keselamatan maklumat JPBD Selangor dalam beberapa aspek berikut:

a) Kerahsiaan (Confidentiality)

Maklumat tidak boleh disebarkan dengan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran.

b) Integriti (Integrity)

Data dan maklumat hendaklah tepat, lengkap dikemaskini dan tidak berlaku sebarang manipulasi. Perubahan sebarang data dan maklumat hanya boleh dilakukan oleh pegawai yang telah diberikan kuasa untuk mengubah maklumat yang berkenaan.

c) Kesahihan (Authenticity)

Punca data dan maklumat hendaklah dari punca yang sah dan tanpa keraguan.

d) Tidak Boleh Disangkal

Data atau maklumat hendaklah dijamin ketepatan, kesahihannya dan tidak boleh disangkal.

e) Kebolehsediaan (Availability)

Data dan maklumat hendaklah sentiasa boleh dicapai pada bila-bila masa.

Penggunaan ICT di agensi kerajaan adalah tertakluk kepada arahan/garis panduan/pekeliling yang dikeluarkan dari semasa ke semasa untuk memperkemaskan jentera kerajaan. Penggunaan ICT juga secara amnya adalah tertakluk kepada undang-undang Kerajaan Malaysia antaranya Electronic Transaction Act 2003, Digital Signature Act 2007, Computer Crime Act 1997, Communications and Multimedia Act 1998, TeleMedicine Act 1997 dan Akta Aktiviti Kerajaan Elektronik 2007.

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan perkara tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam perenggan 53 Arahan Keselamatan.

Semua aset ICT termasuk komputer peribadi dan komputer riba yang dibekalkan kepada pengguna JPBD Selangor adalah untuk kemudahan tugas harian dan merupakan aset mutlak Kerajaan yang boleh ditarik balik pada bila-bila masa jika didapati terdapat penyalahgunaan. Sebarang penyalahgunaan dan kehilangan aset disebabkan kecuaian pegawai akan dikenakan tindakan tata tertib. Sebarang kerosakan atau kegagalan fungsi peralatan ICT perlu dilaporkan melalui borang Aduan Kerosakan Harta Modal Jabatan seperti Lampiran I.

4. KESELAMATAN RANGKAIAN DAN INTERNET

Keselamatan rangkaian merupakan perkara utama dalam pengawalan aset ICT dari dicerobohi oleh pihak luar mahupun dalaman sesebuah organisasi. Keselamatan rangkaian komputer sesebuah organisasi bergantung kepada reka bentuk rangkaian yang betul dan kukuh. Langkah-langkah yang perlu dipertimbangkan adalah:

a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah **diasingkan** untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
b) Peralatan rangkaian hendaklah diletakkan di **lokasi** yang mempunyai ciri-ciri fizikal yang **kukuh dan bebas dari risiko** seperti banjir, gegaran dan habuk;
c) **Capaian** kepada peralatan rangkaian hendaklah **dikawal** dan **terhad** kepada pengguna yang dibenarkan sahaja;
d) Semua peralatan mestilah melalui proses ***Factory Acceptance Check*** **(FAC)** semasa pemasangan dan konfigurasi;
e) ***Firewall*** hendaklah **dipasang** di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem;
f) Semua **trafik keluar dan masuk** hendaklah **melalui *firewall*** di bawah kawalan JPBD Selangor;
g) Semua **perisian *sniffer* atau *network analyser*** adalah **dilarang** dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

h) Memasang perisian ***Intrusion Detection System*** **(IDS)** bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JPBD Selangor;
i) Memasang ***Web Content Filter*** **pada** ***Internet Gateway*** untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
j) Sebarang **penyambungan rangkaian** yang bukan di bawah kawalan JPBD Selangor hendaklah mendapat **kebenaran ICTSO**; dan
k) Memastikan **keperluan perlindungan ICT** adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.

Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan capaian kepada pelbagai maklumat yang terdiri daripada pelbagai bentuk dan format bagi tujuan penyelidikan, analisis, rujukan dan lain-lain. Penggunaan Internet secara tidak bertanggungjawab adalah satu tindakan yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, di samping melemahkan dan mengganggu sistem dan rangkaian ICT JPBD Selangor serta merosakkan imej perkhidmatan awam. Untuk menjamin keselamatan ICT JPBD Selangor pengguna adalah **DILARANG**:

a) Menggunakan kemudahan Internet untuk **tujuan peribadi, aktiviti komersial dan politik**;
b) Memuat naik, memuat turun, menyimpan dan menggunakan **perisian tidak berlesen** (cetak rompak);
c) Menyedia, memuat naik, memuat turun, menyimpan dan menyebarkan sebarang material, teks ucapan, imej atau bahan berunsurkan **lucah, jenayah, pernyataan fitnah atau hasutan, dan bercorak penentangan**;
d) Menggunakan kemudahan **perbincangan awam atas talian** seperti *newsgroup* dan *bulletin board* kecuali mendapat kebenaran dan kelulusan kandungan daripada Ketua Jabatan;
e) Memuat naik, memuat turun, menyimpan dan menggunakan **perisian *peer-topeer* (p2p)** dan **berbentuk hiburan atas talian** seperti permainan elektronik, video dan lagu;
f) Memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepilan fail **melebihi saiz 20MB** yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer; dan
g) Menggunakan **kemudahan modem peribadi** untuk membuat capaian terus ke Internet.

Adalah diingatkan bahawa setiap maklumat yang dikongsi melambangkan imej Kerajaan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan. **Sebarang bentuk pelanggaran larangan di atas adalah menyalahi undangundang Kerajaan Malaysia dan boleh dikenakan tindakan.**

5. KESELAMATAN MEL ELEKTRONIK (E-MEL)

E-mel merupakan satu cara perhubungan yang paling mudah dan murah di antara pengguna dengan pelbagai pihak. Pihak Unit ICT/GIS memandang serius mengenai aspek keselamatan perhubungan melalui e-mel di antara pegawai-pegawai JPBD Selangor, terutama yang melibatkan dokumen terperingkat. **E-mel yang diperuntukkan oleh Jabatan hanya boleh digunakan untuk tujuan rasmi sahaja.**

E-mel rasmi boleh dibahagikan kepada dua kategori berikut:

i. E-mel Rahsia Rasmi

E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan utuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada Terhad, Sulit, Rahsia atau Rahsia Besar.

ii. E-mel Bukan Rahsia Rasmi

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

Semua pegawai JPBD Selangor adalah **diperuntukkan satu akaun e-mel rasmi**, walau bagaimanapun **pewujudan akaun ini bukan secara automatik**. **Permohonan akaun emel baru** perlu dibuat melalui **borang pengurusan e-mel rasmi Jabatan** seperti di Lampiran II. Semua urusan ***reset* kata laluan** dan **penutupan akaun** juga perlu melalui borang ini. Pihak Unit ICT/GIS **tidak akan melayan permohonan yang tidak menggunakan borang** ini kecuali penutupan akaun boleh melalui makluman keluar / masuk kakitangan Jabatan. Penutupan akaun e-mel adalah dibuat seperti berikut:

• Akaun e-mel pengguna yang bersara dihapuskan serta merta;

• Akaun e-mel pengguna yang bertukar ke Jabatan atau Kementerian lain dihapuskan selepas sebulan pertukaran berkuatkuasa; dan

Pengguna terbabit adalah dinasihatkan untuk membuat salinan emel yang perlu sebelum bertukar keluar / bersara (jika perlu).

5.1 Prosedur yang perlu dipatuhi

Bagi memastikan penggunaan e-mel dapat beroperasi dengan sempurna dan berkesan, pengguna adalah **DILARANG**:

a) Menggunakan kemudahan e-mel rasmi Jabatan untuk **tujuan peribadi, aktiviti komersial dan politik**;
b) **Menggunakan akaun e-mel orang lain** atau berkongsi e-mel atau memberi kata laluan akaun e-mel kepada orang lain;
c) Menghantar emel rasmi **menggunakan akaun selain akaun emel rasmi** Jabatan;
d) **Membuka e-mel dari penghantar yang tidak dikenali** yang berkemungkinan mengandungi virus;
e) **Menyebarkan kod perosak** seperti virus, *worm*, *Trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;
f) **Menyebarkan gambar-gambar lucah, e-mel berunsurkan fitnah, perkauman, gangguan seksual** atau yang berkaitan dengannya;
g) **Membenarkan pihak ketiga untuk menjawab e-mel** kepada penghantar asal bagi pihaknya; dan
h) Membuka e-mel yang mengandungi fail kepilan (attachment file) seperti *.scr, *.com, *.exe, *.dll, *.pif, *.vbs, *.bat, *.asd, *.chm, *.ocx, *.hlp, *.hta, *.js, *.shb, *.shs, *.vb, *.vbe, *.wsf, *.wsh, *.reg, *.ini, *.diz, *.cpp, *.cpl, *.vxd, *.sys dan *.cmd. Ia berkemungkinan akan menyebarkan virus apabila dibuka.

5.2 Pengendalian E-mel Rahsia Rasmi

Pengurusan maklumat terperingkat adalah tertakluk di bawah peruntukan Akta Rahsia Rasmi 1972. Perkara–perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan e-mel rahsia rasmi iaitu:

a) Maklumat terperingkat sebolehnya **tidak di e-mel kecuali perlu**;
b) **Penyulitan** mesti dilakukan ke atas semua e-mel rahsia rasmi yang dihantar, diterima dan disimpan;
c) Penerima e-mel rahsia rasmi mesti **mengesahkan kesahihan dokumen** apabila ditandatangani secara digital oleh pengirim;
d) Penerima mesti **membuat akuan penerimaan** e-mel rahsia rasmi sebaik sahaja menerimanya;
e) E-mel rahsia rasmi bertanda **Rahsia Besar dan Rahsia tidak boleh dimajukan** kepada pihak lain. Sementara e-mel bertanda **Sulit dan Terhad** yang hendak dimajukan kepada pihak lain **memerlukan izin daripada pemula dokumen**; dan
f) E-mel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan perlulah **dihapuskan secara kekal** dari folder 'Deleted Items' atau dengan melaksanakan 'Empty Trash'.

5.3 Tanggungjawab Pengguna

Pengguna hendaklah mematuhi tatacara penggunaan e-mel yang telah ditetapkan agar keselamatan ke atas penggunaannya terus terjamin. **Peranan dan tanggungjawab pengguna** adalah seperti berikut:

a) **Tidak mendedahkan kata laluan** kepada sesiapa walaupun diminta sama ada melalui e-mel atau medium lain;
b) Menggunakan **webmail JPBD Selangor** jika ingin membuat **capaian e-mel rasmi** Jabatan. Sila layari http://www.jpbdselangor.gov.my/webmail;
c) Membuat **permohonan akaun e-mel baru, penutupan akaun emel sedia ada** dan ***reset* kata laluan** menggunakan **borang pengurusan emel rasmi Jabatan** seperti di Lampiran II;
d) Memastikan kata laluan mengandungi **kombinasi nombor, huruf dan simbol** dengan **minimum lapan (8) aksara**;
e) Membuat **penukaran kata laluan setiap 3 bulan** bagi tujuan keselamatan;
f) Memastikan **saiz fail kepilan** (attachment file) termasuk kandungan e-mel yang dibenarkan untuk penghantaran adalah **tidak melebihi 20MB**;
g) Melakukan penyelenggaraan akaun dengan kerap agar **saiz storan tidak melebihi 1MB**. Penyelenggaraan boleh dilakukan dengan memadam atau menyalin mana-mana e-mel yang telah dibaca atau diambil tindakan. Ini bertujuan untuk menjamin prestasi server e-mel;
h) **Mencetak dan mendokumenkan semua e-mel yang penting** untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada cakera keras komputer;
i) Membuat salinan dan menyimpan fail kepilan ke dalam satu *folder* berasingan dari setiap e-mel yang penting bagi tujuan ***backup*** jika berlaku sebarang masalah kepada cakera keras komputer. Sila rujuk Lampiran III;
j) Melakukan **imbasan ke atas semua fail dan fail kepilan** bagi mengenal pasti fail yang diserang virus dengan perisian anti virus yang diguna pakai Jabatan;
k) Memastikan kemudahan e-mel **digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja** supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan segera dapat diambil ke atasnya;
l) Untuk keselamatan **dokumen rahsia rasmi dan maklumat terperingkat** yang dihantar melalui e-mel **disulitkan** terlebih dahulu;
m) Menggunakan ***carbon copy* (cc)** apabila e-mel tersebut perlu dimaklumkan kepada penerima lain. Sebolehnya penggunaan ***blind carbon copy* (bcc) dielakkan** kerana dilihat sebagai ingin menyembunyikan sesuatu; dan
n) **Memaklumkan** dengan segera nama **kakitangan JPBD Selangor yang bertukar atau berhenti kepada Unit ICT/GIS** agar akaun e-mel mereka dapat dikemaskini.

Pihak Unit ICT/GIS tidak akan bertanggungjawab ke atas e-mel yang hilang bagi pengguna yang tidak mematuhi polisi penggunaan e-mel.

6. KESELAMATAN DARI ANCAMAN VIRUS DAN *SPYWARE*

Serangan virus komputer dan *spyware* boleh menyebabkan kerosakan ke atas peralatan komputer, kehilangan atau kerosakan maklumat penting dan boleh disebarkan tanpa disedari oleh pengguna.

Untuk meningkatkan lagi tahap keselamatan maklumat dan infrastruktur ICT JPBD Selangor dari ancaman virus dan *spyware*, semua pengguna dikehendaki **mengambil langkahlangkah keselamatan** berikut:

a) Sentiasa **melakukan imbasan dan nyah virus** (virus scanning) ke atas **setiap media storan luar** (disket / cakera padat / external hard disk / pendrive dsb.) untuk mengesahkan bahawa ianya adalah bebas daripada sebarang virus atau *spyware*. Dengan cara ini, pengguna dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus;
b) Menggunakan **perisian anti virus yang sah dan diperoleh oleh Jabatan**. Maklumat terkini berkaitan serangan virus dan penyelesaian boleh didapati dengan melayari laman web perisian anti virus tersebut (contohnya http://www.asetnod32.com);

c) **Tidak melayari sebarang laman web berunsur lucah** yang mana sudah diketahui umum mempunyai banyak *spyware* yang boleh menyebabkan penurunan prestasi komputer pengguna selain daripada boleh mencuri maklumat yang terkandung di dalam komputer pengguna;
d) Memastikan setiap komputer dan *notebook* yang digunakan dilakukan **proses imbasan dan nyah virus sekerap yang mungkin**. Ini bertujuan untuk memastikan bahawa semua komputer yang digunakan adalah bebas daripada sebarang virus; dan
e) **Memaklumkan serangan virus dan *spyware* kepada Unit ICT/GIS** supaya tindakan lanjut dapat diambil.

7. KESELAMATAN ID PENGGUNA DAN KATA LALUAN (*PASSWORD*)

ID pengguna dan kata laluan merupakan kata kunci atau *pin number* yang menjadi hak individu dan menjadi rahsia dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga ID pengguna dan kata laluan masing-masing dengan teliti agar tidak dicerobohi oleh pengguna lain. Bagi menjamin keselamatan ID pengguna dan kata laluan, pengguna hendaklah **mengambil langkah-langkah keselamatan** berikut:

a) ID pengguna yang diberikan bagi setiap sistem aplikasi adalah **unik** bagi setiap pengguna dan akan menggunakan sama ada **nombor kad pengenalan** pengguna **atau nama** pengguna;
b) ID pengguna dan kata laluan bagi satu-satu sistem aplikasi **tidak dibenarkan sama**;
c) Aplikasi sebolehnya mempunyai **ciri log keluar automatik** selepas masa tidak aktif (contohnya selepas 15 minit);
d) **Rahsiakan ID pengguna dan kata laluan**. ID pengguna dan kata laluan hendaklah **dihafal dan tidak disalin** atau disimpan di dalam mana-mana media seperti buku catatan, disket, CD dan sebagainya kerana dikhuatiri akan diketahui dan disalah gunakan oleh mereka yang tidak bertanggungjawab;
e) Menggunakan **kata laluan berbeza daripada ID pengguna**;
f) Menggunakan **kata laluan sekurang-kurangnya lapan (8) aksara**;
g) Menggunakan kata laluan yang kukuh dengan **kombinasi nombor, huruf dan simbol** (*contoh: p@5$w0Ri)*);
h) **Menukar** kata laluan setiap **tiga (3) bulan sekali**. Bagi e-mel Jabatan, pengguna akan di*prompt* secara automatik untuk membuat penukaran kata laluan setiap 90 hari;
i) **Melaporkan kepada pegawai keselamatan ICT Jabatan** sekiranya kata laluan telah **dicerobohi atau disyaki telah dicerobohi**. Kata laluan sedia ada akan diubah serta merta; dan
j) ID pengguna dan kata laluan bagin sistem aplikasi Jabatan akan ditarik balik serta merta setelah pengguna bertukar/bersara.

Sila rujuk Lampiran IV untuk mengetahui cara-cara untuk mengubah kata laluan e-mel.

8. KESELAMATAN FIZIKAL KOMPUTER PERIBADI DAN KOMPUTER RIBA

Keselamatan fizikal meliputi komputer peribadi, komputer riba dan perkakasan terlibat seperti cakera keras, pencetak, pengimbas dan lain-lain. Pengguna komputer peribadi dan riba Jabatan hendaklah sentiasa **mematuhi peraturan keselamatan** berikut:

a) Setiap komputer mestilah **mempunyai kata laluan**;
b) Pengguna dinasihatkan supaya membuat ***backup*** **semua dokumen dan data penting** yang disimpan di cakera keras (hard disk) komputer **ke media storan lain** secara berkala sekerap mungkin bagi langkah pemulihan sekiranya berlaku kerosakan;
c) **Pengemaskinian *Microsoft Windows, patches* dan *service pack*** yang terkini mestilah dilakukan ke atas setiap komputer dari semasa ke semasa. Sila hubungi Unit ICT/GIS untuk bantuan;
d) Setiap komputer mestilah **mempunyai perisian antivirus yang diguna pakai di Jabatan**;
e) Pengguna **dilarang sama sekali mengubah atau meminda** "***Computer Name***" dan "***Description***" di dalam komputer;
f) **Jangan** biarkan komputer berada di atas talian (***on-line***) **jika tidak digunakan**, dan ***log off*** komputer **sebelum meninggalkan pejabat**;
g) Pastikan **komputer pejabat** hanya digunakan **untuk urusan pejabat** sahaja dan tidak digunakan oleh orang lain yang tidak berkenaan;
h) Dilarang menggunakan alat penyambung kuasa elektrik bagi pelbagai peralatan. Bekalan kuasa elektrik yang tidak stabil akan merosakkan komputer. Gunakan kemudahan ***Uninterruptible Power Supply (UPS)*** atau ***Automatic Voltage Regulator (AVR)*** untuk memastikan bekalan elektrik sentiasa dibekalkan mengikut spesifikasi keperluan komputer atau komputer riba;
i) Pastikan **bekalan atau punca elektrik ditutup** semasa pemasangan atau penyambungan peralatan komputer dan aksesorinya atau setelah selesai menggunakan komputer;
j) Pastikan **komputer tidak terdedah** secara terus kepada **pancaran matahari/haba** dan **elakkan** komputer daripada **kawasan tarikan kuasa magnet/kuasa voltan** yang tinggi;
k) Pastikan komputer diletakkan di tempat **dingin dan kering** persekitarannya serta di tempat yang selamat;
l) **Rehatkan komputer** jika digunakan secara berterusan;
m) Tamatkan "***not responding***" dengan menekan kekunci ***Ctrl-Alt-Del*** jika sebarang program komputer tidak berfungsi (*hang*);
n) Pastikan komputer mempunyai ***system date & time*** yang betul untuk tujuan audit dan penghantaran e-mel;
o) Sentiasa keluar dari Windows atau **menutup komputer** dengan cara yang betul bagi mencegah ralat sistem iaitu **klik *Start -> Shut Down***. **DILARANG** sama sekali **menutup komputer secara fizikal** iaitu dengan menutup suis atau mencabut plug atau sebagainya;
p) **DILARANG menghentak/mengetuk** dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer;
q) Pastikan **komputer riba disimpan di dalam almari berkunci** setelah digunakan;
r) Pengguna dinasihatkan **membuat *basic maintenance*** seperti clean up, defragmentation dan scan disk secara berkala setiap bulan; dan
s) **Tidak dibenarkan membaiki sendiri komputer** jika terdapat sebarang masalah atau kerosakan. Sila hubungi Unit ICT/GIS untuk bantuan.

Sebarang **kehilangan dan apa juga bentuk penyalahgunaan penggunaan aset ICT** Kerajaan terutama komputer **boleh dikenakan tindakan**, dan **kemudahan boleh ditarik balik pada bila-bila masa**.

8.1. Kemudahan komputer di bilik mesyuarat dan kaunter

Pengguna perlu mematuhi peraturan penggunaan seperti berikut:

a) Memadamkan dokumen yang disimpan di dalam komputer selepas selesai digunakan;
b) Tidak membuat sebarang instalasi perisian kepada komputer kecuali dengan kebenaran Unit ICT/GIS;
c) Memastikan komputer di *shut down* dan semua suis dimatikan selepas tamat penggunaan.

9. KESELAMATAN PUSAT DATA

Untuk memastikan server penting sentiasa selamat daripada pencerobohan atau sebarang ancaman dan membolehkan ia dicapai sepanjang masa, semua server hendaklah diletakkan di dalam pusat data yang mempunyai kemudahan keselamatan, penyaman udara khas, dan kemudahan perlindungan suhu dan kebakaran. Pusat data juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti firewall dan UPS. Antara langkah yang boleh dilaksanakan bagi melindungi pusat data ialah:

a) Dilengkapi pintu akses yang kukuh;
b) Hanya pegawai Unit ICT/GIS yang mempunyai akses sahaja yang dibenarkan masuk;
c) Pengguna lain / pihak ketiga perlu memohon kebenaran masuk ke pusat data dari Pegawai ICTSO rujuk lampiran vi.
d) Setiap server mestilah dilabelkan penggunaannya bagi memudahkan pentadbir menjalankan tugas;
e) Pastikan pusat data sentiasa bersih dan server serta peralatan lain tidak terdedah kepada habuk;
f) Penghawa dingin mestilah berfungsi dengan baik di mana suhu di dalam lingkungan 19.5°C dan kelembapan di paras 50.7%;
g) Semua peralatan keselamatan, UPS dan penghawa dingin mestilah diselenggarakan sekerap yang mungkin;
h) Alat pemadam kebakaran perlu diletakkan di tempat yang mudah diakses; dan
i) Kertas cetakan yang tidak digunakan perlu diricih.

10. KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA

Data dan maklumat sistem aplikasi yang telah dibangunkan dan beroperasi merupakan aset yang penting dan perlu dilindungi sebaik mungkin demi menjamin keselamatannya.

Antara langkah yang telah dikenalpasti dan dilaksanakan bagi melindungi perisian sistem dan pangkalan data adalah proses *backup* dan *restore*. Proses ini dibuat sekiranya perkara berikut berlaku:

• Kegagalan server berfungsi

• Kerosakan fizikal cakera keras

• Masalah dalam pemprograman

a) *Backup file* perlu dilabel dengan betul agar tidak berlaku kesalahan pemadaman;
b) *Backup* keseluruhan data dan aplikasi di buat pada setiap malam untuk semua server berpandukan prosedur *backup* yang telah ditetapkan;
c) *Backup* atau salinan data ke dalam media storan perlu dilakukan setiap hari untuk mengelakkan kehilangan data sekiranya berlaku kerosakan cakera keras;
d) Pelabelan nama fail yang disalin (*backup*) untuk memudahkan carian fail dari masa ke semasa;
e) *Backup* sistem aplikasi perlu dibuat sekurang-kurangnya sekali bagi setiap keluaran versi terbaru dari masa ke semasa mengikut peraturan yang ditetapkan semasa perisian itu dibangunkan atau diperolehi atau mengikut garis panduan yang dikeluarkan dari masa ke semasa. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam menentukan kekerapan *backup*.
f) *Backup* untuk data dan sistem aplikasi dicadangkan dibuat dalam tiga(3) salinan dan setiap satu disimpan di lokasi yang berlainan. Lokasi tersebut adalah:
    - Lokasi di mana sistem tersebut beroperasi

- Lokasi off-site pertama – di bilik pegawai tingkat 17 Bangunan Darul Ehsan
- Lokasi off-site kedua – di bangunan lain yang berdekatan atau mana-mana Jabatan kerajaan lain yang berdekatan dan mempunyai kemudahan untuk menyimpan media backup. Penetapan lokasi simpanan *backup* ini adalah untuk memastikan data-data kritikal/penting masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal, contohnya jika berlaku bencana seperti kebakaran, banjir dan sebagainya.

10.1. Pelan Pemulihan Bencana

Data-data kritikal disalin (backup) ke dalam pita dan disimpan di dalam pusat data, di samping itu pendua bagi data-data tersebut telah dihantar dan disimpan di JPBDSM sebagai salah satu pelan pemulihan bencana. Keadaan ini dilakukan bagi memastikan data-data kritikal masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal di pusat data, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebagainya.

11. TATACARA PEMINJAMAN PERALATAN ICT

Pendaftaran aset ICT buat masa ini adalah di bawah Bahagian Pentadbiran dan Kewangan. Oleh itu **Bahagian tersebut adalah bertanggungjawab memastikan** supaya segala peralatan ICT termasuk projektor, komputer riba, PC, pencetak dan aksesori yang berkaitan seperti plug extension, kabel komputer dan sebagainya yang dipinjam atau dibawa keluar atau masuk daripada premis pemunya (contohnya peralatan pinjaman Unit ICT/GIS) adalah **tertakluk di bawah prosedur** berikut:

a) Semua pinjaman peralatan ICT perlu **melalui permohonan rasmi secara memo atau emel** kepada Pegawai Aset;
b) Setiap pengguna dikehendaki **mengisi dan menandatangani borang peminjaman peralatan ICT** seperti Lampiran V dan **KEW. PA-6**;
c) Peralatan ICT yang dipinjam dan borang tersebut perlu dikembalikan setelah selesai menggunakannya untuk semakan dan simpanan pihak pemunya;
d) Adalah menjadi **tanggungjawab peminjam** untuk:
    - **menjaga dengan baik** peralatan ICT agar tidak berlaku kerosakan atau kehilangan;
    - memastikan kesemua peralatan ICT **dikembalikan dengan sempurna, lengkap dan selamat**;
    - memastikan **semua dokumen yang disimpan di dalam *hard disk*** notebook yang dipinjam **dipindahkan** ke storan lain sebelum dipulangkan, dan **dipadam** daripada *hard disk* notebook yang dipinjam sebelum dipulangkan. Pihak Unit ICT/GIS akan membuat *housekeeping* setiap minggu semua notebook pinjaman dan tidak akan bertanggungjawab sekiranya peminjam gagal memindahkan dokumen ke storan lain;
    - memastikan semua **media storan elektronik luar** (disket / pen drive / external hard disk dsb.) yang disambung ke notebook pinjaman **dinyah virus** (scan) terlebih dahulu sebelum dibuka;
    - **melaporkan sebarang kerosakan dan kegagalan** peralatan ICT **kepada** Unit ICT/GIS dengan segera melalui borang Aduan Kerosakan Aset Jabatan; dan
    - **melaporkan sebarang kehilangan** peralatan ICT yang dipinjam **kepada pemunya** dengan segera supaya tindakan yang berkaitan dapat diambil.

12. TATACARA PENGURUSAN MEDIA STORAN

Disket / CD / pen drive merupakan antara media storan elektronik luar yang digunakan untuk menyimpan data atau kandungan fail. Untuk menjamin keselamatan kandungan, pengguna adalah dinasihatkan supaya **mengikuti langkah-langkah berikut**:

a) Media storan yang diperolehi adalah **untuk tujuan rasmi** sahaja;
b) Setiap media storan perlulah **dilabelkan mengikut Bahagian/Unit/Nama**;
c) Setiap **pen drive** juga perlulah **dilabelkan (Volume label)** untuk memudahkan pengecaman hakmilik. Sila rujuk Lampiran VI untuk cara pelabelan;

d) Media storan yang mengandungi maklumat sulit/ rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad atau Sulit dan mestilah disimpan di tempat yang selamat. Bagi fail yang diklasifikasikan sebagai **Rahsia/Sulit**, pengguna dinasihatkan untuk **mewujudkan kata laluan bagi fail-fail** tersebut. Cara-cara untuk mewujudkan kata laluan boleh didapati di Lampiran VII ;

e) Pengguna adalah **DILARANG membawa keluar atau memberi media storan yang mengandungi maklumat rahsia rasmi kepada orang lain**. Ini adalah untuk mengelakkan daripada berlakunya kebocoran rahsia;

f) Pengguna hendaklah memastikan **saiz fail** yang disimpan di dalam Media storan **tidak melebihi ruang storan** (1.44MB bagi disket) yang diperuntukkan dan mengutamakan penyimpanan fail yang perlu sahaja. Sekiranya perlu disarankan untuk melakukan **kaedah pemampatan** (compress) untuk

g) mengurangkan saiz fail;

h) Media storan yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadam (delete) sebelum digunakan untuk tujuan yang lain;

i) Bagi penggunaan pen drive, ia mestilah **dikeluarkan daripada system dengan cara yang betul**. Pengguna dilarang mengeluarkan pen drive dari USB dengan cara terus. Sila rujuk Lampiran VIII.

10.1. Pemusnahan Media Storan

Kaedah pemusnahan media adalah seperti berikut:

a) Media magnetik

i. Mendedahkan media kepada medan magnet yang kuat..

ii. Format semula bagi memadamkan semua data dan diguna pakai semula.

h) Media optic

iii. Kaedah pemusnahan secara fizikal iaitu memotong, menggunting dsb.

iv. Format semula *rewritable optical disk* bagi memadamkan semua data dan diguna pakai semula.

13. KHIDMAT NASIHAT

Sebarang kemusykilan atau pertanyaan berkaitan Dasar Keselamatan ICT ini, sila hubungi Jawatankuasa Keselamatan ICT Jabatan.

En. Mohd Rozuwan Ab Ilah (rozuwan@jpbdselangor.gov.my)

En. Muhamad Azuwan Abdul Rahman (muhamad.azuwan@jpbdselangor.gov.my)

14. PENUTUP

Secara ringkasnya, keselamatan ICT JPBD Selangor perlu dilaksanakan secara menyeluruh dan memerlukan kerjasama semua pengguna. Aspek keselamatan ICT merupakan tanggungjawab bersama dan tidak hanya dikhususkan kepada satu pihak sahaja. Maklumat penting JPBD Selangor perlu sentiasa di dalam keadaan boleh dipercayai dan boleh dicapai pada bila-bila masa tanpa sebarang keraguan.

Lampiran i

Borang Aduan Kerosakan Aset Alih Kerajaan **KEW.PA-9**

KEW.PA-9

BORANG ADUAN KEROSAKAN ASET ALIH KERAJAAN

Bahagian 1 (Untuk diisi oleh Pegawai Aset)

1. Jenis Aset :
2. Keterangan Aset :
3. Nombor Siri Pendaftaran :
4. Kos penyelenggaraan terdahulu(jika ada) :
5. Pengguna Terakhir :
6. Tarikh Kerosakan :
7. Perihal kerosakan :

8. Syor Pegawai Aset

Nama : .....
Jawatan : .....
Tarikh : .....

Bahagian II (Keputusan Ketua Jabatan)

Diluluskan / tidak Diluluskan*

.....
Tandatangan
Nama : .....
Jawatan : .....
Tarikh : .....

Nota: * Potong mana yang berkenaan.

Lampiran ii

Borang mewujudkan akaun email Jabatan

Borang Pengurusan Emel

A. MAKLUMAT PERMOHONAN (DIISI OLEH PEMOHON)

1) Nama :
2) Jawatan :
3) Gred :
4) No. Telefon Pejabat :
5) No. Telefon Peribadi :
6) Jenis Permohonan :

☐ Permohonan Baru
☐ Hapus (Sebab: _____)
☐ Reset Password (Sebab: _____)

Dengan ini saya mengesahkan bahawa kesemua maklumat yang diberi adalah benar. Saya berjanji akan menggunakan emel Jabatan mengikut yang digariskan PKPA Bil. 1 Tahun 2003.

Tanda tangan Pemohon :

Nama dan cop jawatan :

Tarikh :

B. MAKLUMAT PELAKSANAAN (DIISI OLEH UNIT ICT/GIS)

☐ Diluluskan
☐ Ditolak (Sebab: _____)

Alamat emel yang diwujudkan :

Kata laluan sementara :

Pentadbir emel : Tarikh :

Peringatan:

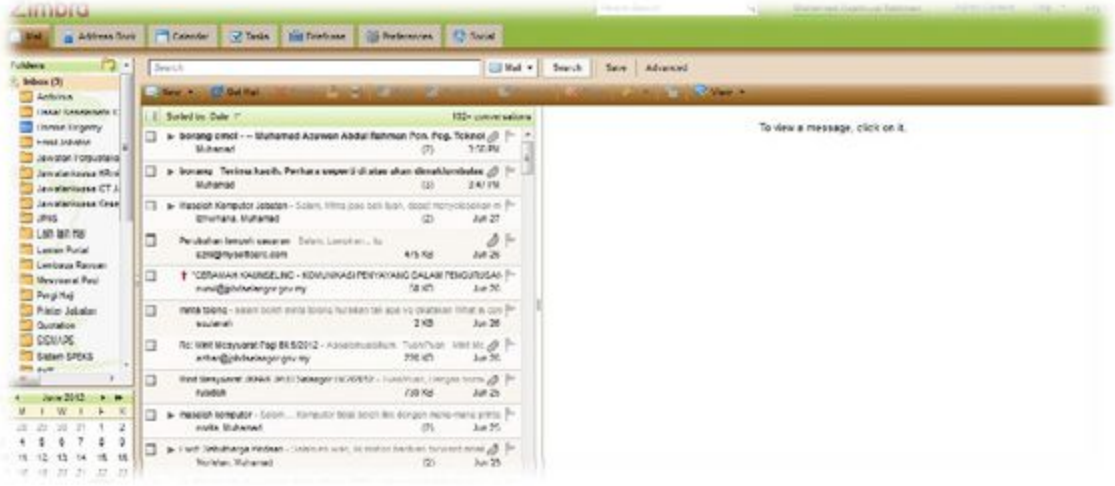
1. *Penggunaan emel jabatan adalah tertakluk di bawah Pekeliling Kemajuan Perkhidmat Awam Bil. 1 Tahun 2003 dan Dasar Keselamatan ICT Jabatan.*
2. *Emel yang disediakan hendaklah digunakan untuk tujuan rasmi sahaja.*
3. *Menggunakan emel Jabatan bukan untuk tujuan lain seperti menyedia dan menghantar maklumat berulang-ulang yang berupa gangguan, menyedia, menerima serta memuat turun dan menyimpan maklumat yang mengandungi unsur-unsur lucah atau sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan, atau menggunakan emel untuk tujuan komersial, politik, perjudian dan sebagainya.*
4. *Kegagalan mematuhi kepada perkara tersebut di atas membolehkan tuan-puan diambil tindakan.*

Lampiran iii

Cara membuat salinan (backup) emel zimbra Jabatan.

Langkah 1

Buka paparan e-mel masing-masing.

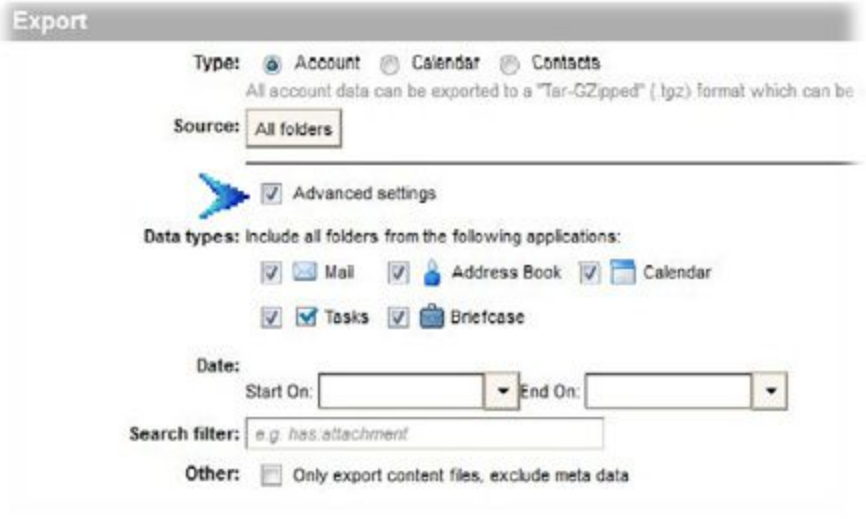


Langkah 2

Klik pada *tab* Preferences, *select* pada tajuk Import / Export pada menu sebelah kiri.

Langkah 3

Tandakan *tick* pada ruangan Advanced setting untuk mengetahui maklumat yang di salin atau ingin membuat masa pada salinan tersebut.



Langkah 4

Tekan butang export pada sebelah kanan bawah anda.

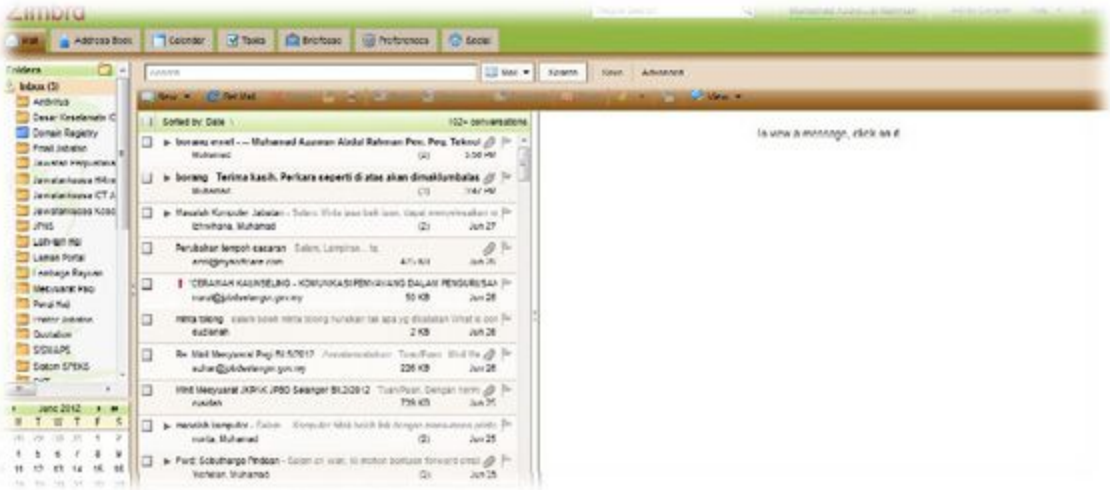
Tekan butang save untuk arahan seterusnya. Selesai.

Lampiran iv

Cara untuk menukar kata laluan emel Jabatan.

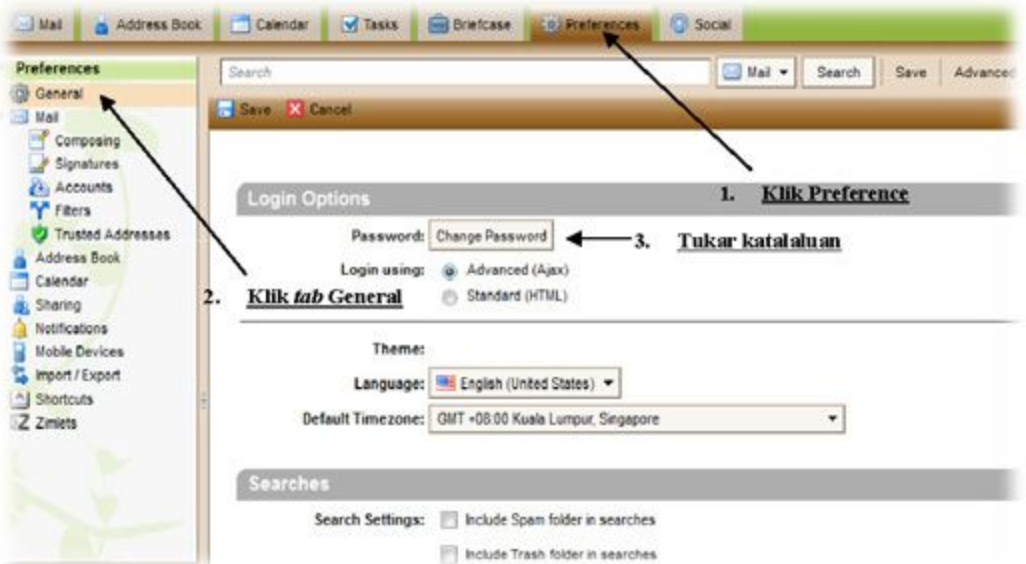
Langkah 1

Buka paparan emel Jabatan.



Langkah 2

Klik pada *tab* General, diruangan Login Option tekan butang *Change Password*.



Langkah 3

Paparan seperti dibawah adalah anda perlu memasukkan katalaluan lama diiringi katalaluan baru sebanyak dua kali untuk dikenal pasti oleh sistem. Kemudian tekan butang *Change Password*.
Untuk menukar katalaluan anda perlu mamatuhi syarat keselamatan iaitu:

a) Minimum panjang katalaluan adalah 7
b) Maximum panjang katalaluan adalah 64
c) Minimum huruf besar (wajib) adalah 1
d) Minimum nombor (wajib) adalah 1

Jika anda mematuhi syarat keselamatan seperti diatas, maka anda telah Berjaya menukar katalaluan tersebut.

Selesai.

Lampiran v

Tatacara bilik server Jabatan.

TATACARA MEMASUKI BILIK SERVER JABATAN PERANCANGAN BANDAR DAN DESA NEGERI SELANGOR

1) **Pegawai/individu hendaklah berjumpa Pegawai Keselamatan ICT (ICTSO);**
2) **Meminta kebenaran untuk memasuki bilik server atas sesuatu tujuan rasmi/kerja;**
3) **Pegawai Keselamatan ICT (ICTSO) akan mempertimbangkan kerja-kerja yang hendak dilakukan;**
4) **Jika kerja-kerja tersebut tidak berkaitan atau tidak memerlukan untuk memasuki bilik server maka permohonan akan di tolak;**
5) **Pegawai Keselamatan ICT (ICTSO) akan mengiringi pegawai/individu tersebut ke bilik server dan membuka pintu;**
6) **Pegawai/individu wajib mengisi log keluar / masuk di dalam buku log yang telah disediakan.**
7) **Pegawai/individu mestilah mendapatkan pengesahan oleh Pegawai Keselamatan ICT (ICTSO) sebelum meninggalkan bilik server.**

JPBD SELANGOR | **PROSEDUR DAN PERATURAN AM BILIK SERVER** 1

CARTA ALIR TATACARA MEMASUKI BILIK SERVER

Carta Alir Bilik Server JPBD Selangor

Disediakan oleh,

MOHD ROZUWAN BIN AB'LLAH
PEGAWAI KESELAMATAN ICT (ICTSO)

Disahkan oleh,

DATO' MOHD.JAAFAR BIN MOHD.ATAN
KETUA PEGAWAI MAKLUMAT (CIO)

Tarikh kuatkuasa pada: 12.2.2010

PERATURAN AM BILIK SERVER JABATAN PERANCANGAN BANDAR DAN DESA NEGERI SELANGOR

1) **Memastikan kebenaran diperolehi dari Pegawai Keselamatan ICT (ICTSO) untuk memasuki bilik server.**

2) **Memastikan individu yang diberi kebenaran masuk bertanggungjawab diatas sebarang kejadian.**

3) **Memastikan pintu sentiasa ditutup dan dikunci.**

4) **Memastikan bilik server sentiasa bersih.**

5) **Memastikan penghawa dingin sentiasa berfungsi dan suhu di bawah 16 darjah Celsius.**

6) **Memastikan Uninterruptable Power Supply (UPS) dalam keadaan baik dan stabil.**

7) **Memastikan alat pencegah kebakaran (CO2) dalam keadaan baik dan tidak luput.**

8) **Memastikan perkara-perkara berikut dipatuhi ketika berada didalam bilik server:**

   a) **Dilarang menghisap rokok;**
   b) **Dilarang membawa makanan dan minuman;**
   c) **Dilarang membawa alat mudah terbakar.**

Disediakan oleh,

MOHD ROZUWAN BIN AB'LLAH
PEGAWAI KESELAMATAN ICT (ICTSO)

Disahkan oleh,

DATO' MOHD JAAFAR BIN MOHD.ATAN
KETUA PEGAWAI MAKLUMAT (CIO)

Tarikh kuatkuasa pada: 12.2.2010

Lampiran vi

Borang Daftar Pergerakan Harta Modal dan Inventori **KEW.PA-6**

KEW.PA-6

DAFTAR PERGERAKAN HARTA MODAL DAN INVENTORI

Jenis	
Jenama dan Model	
No. Siri Pembuat	
No. Siri Pendaftaran	

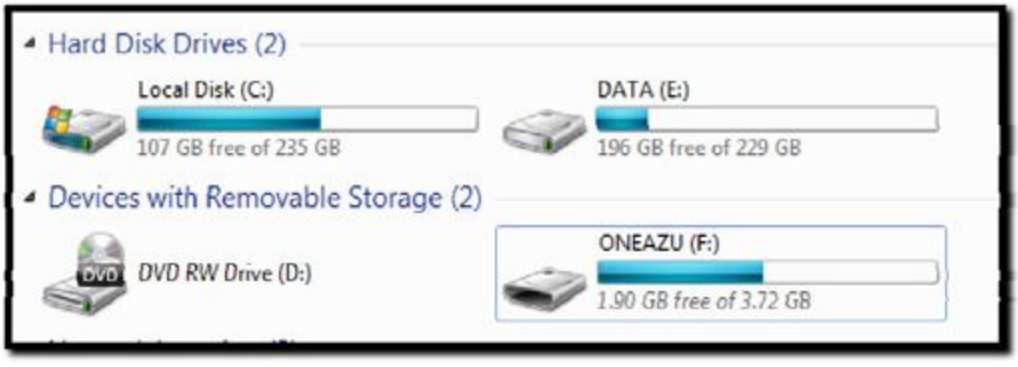
Bil	Nama Peminjam	Tarikh		Tandatangan Peminjam	Pegawai Pengeluar				Catatan
		Dikeluarkan	Jangka Dipulangkan		Ketika Dikeluarkan		Ketika Dipulangkan		
					Tandatangan	Tarikh	Tandatangan	Tarikh	

Lampiran vii

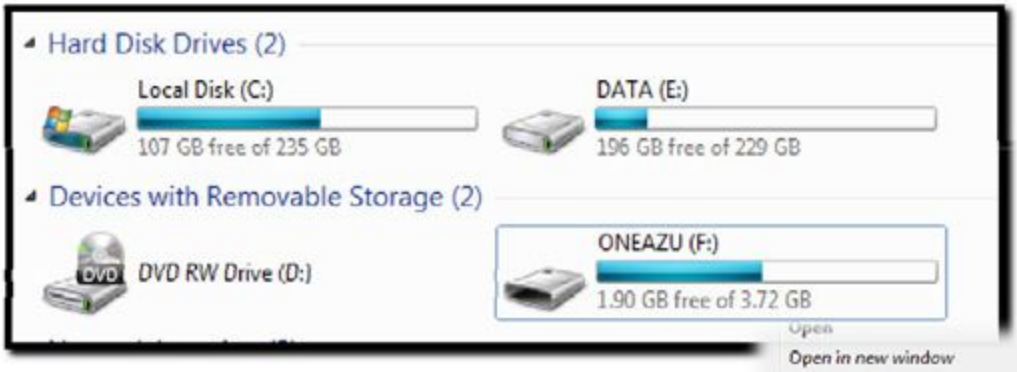
Cara untuk membuat pelabelan pada *thumb drive*.

Langkah 1

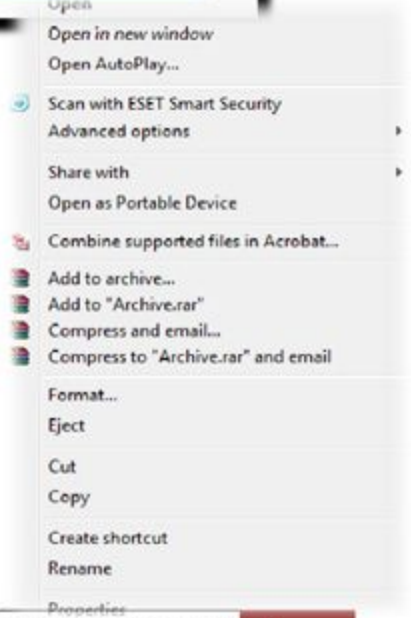
Buka paparan *My Computer* anda. Pastikan anda melihat dimana ruangan *thumdrive* anda.



Langkah 2



Klik kanan pada tetikus anda dan pilih *Rename*.



Tulis nama anda pada ruangan [TULIS NAMA] seperti diatas. Kemudian tekan buatang *Enter*.

Selesai.

Lampiran viii

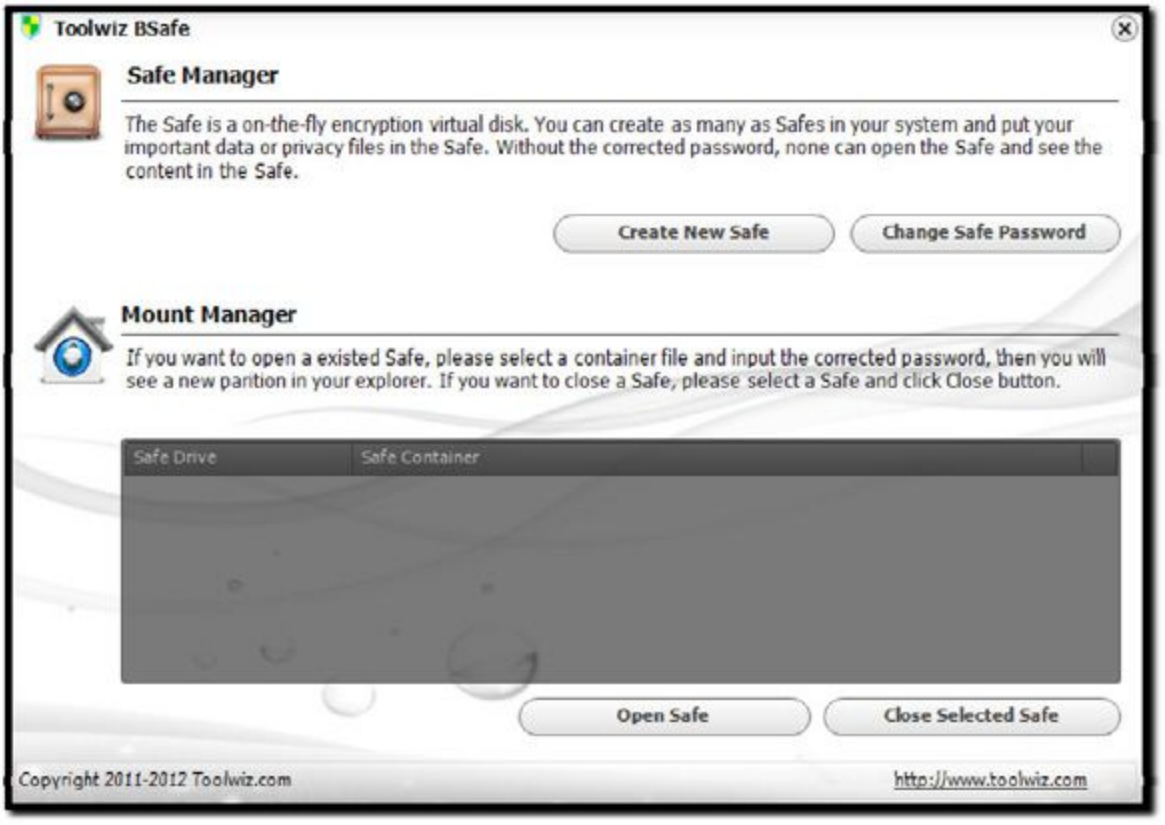
Cara mewujudkan zon keselamatan data.

Langkah 1

Buat pemasangan perisian *Toolwiz BSafe*

Langkah 2

Buka perisian tersebut seperti dibawah ini.

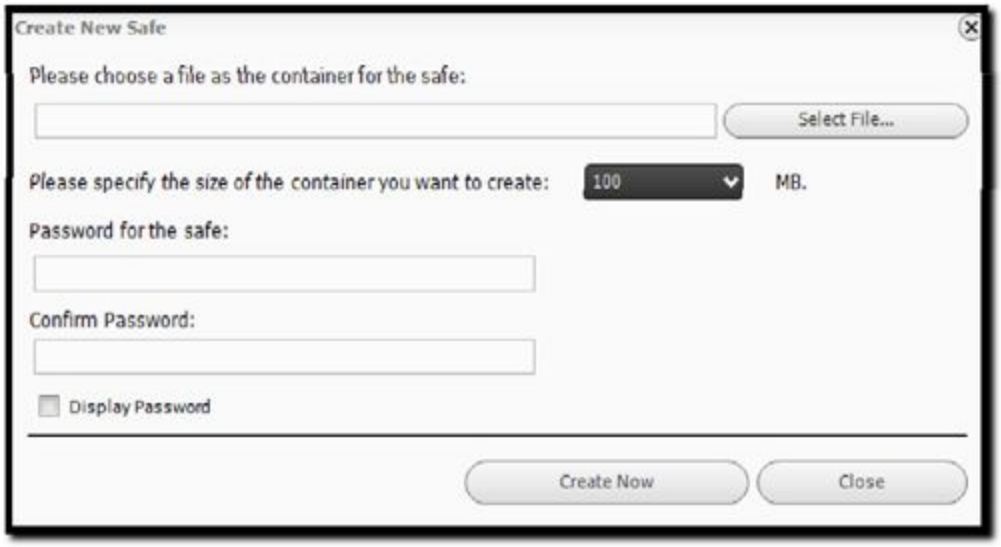


Langkah 3

Tekan butang *Create New Safe* untuk mewujudkan satu lokasi keselamatan didalam komputer anda.

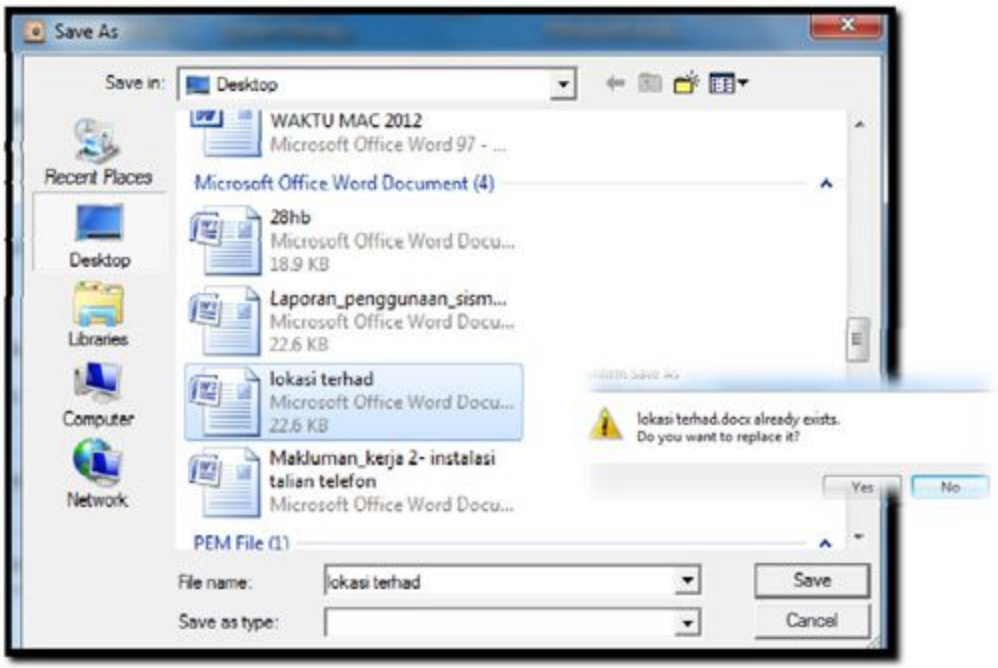
Langkah 4

Tekan butang *Select File*.. untuk memilih dokumen sebagai destinasi ruang keselamatan data. Anda juga boleh menentukan ruang keselamatan anda dibahagian *MB*. Kemudian masukkan katalaluan.



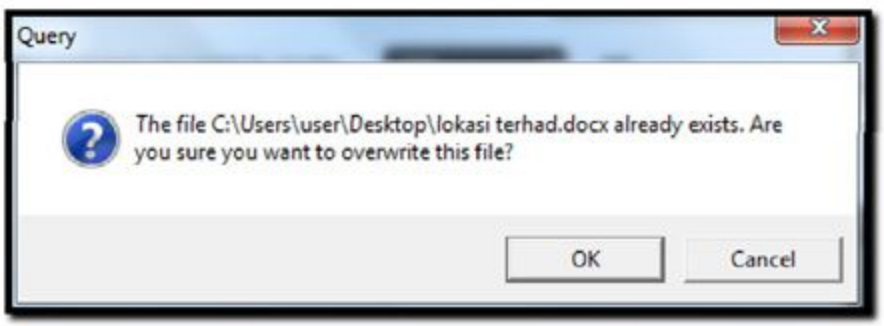
Langkah 5

Gambar rajah dibawah adalah contoh memilih dokumen sebagai ruang keselamatan data. Pilih dokumen tersebut dan tekan butang *Save*. Satu dialog box akan keluar dan meminta anda utk *replace* dokumen tersebut. Pilih *Yes* untuk teruskan.



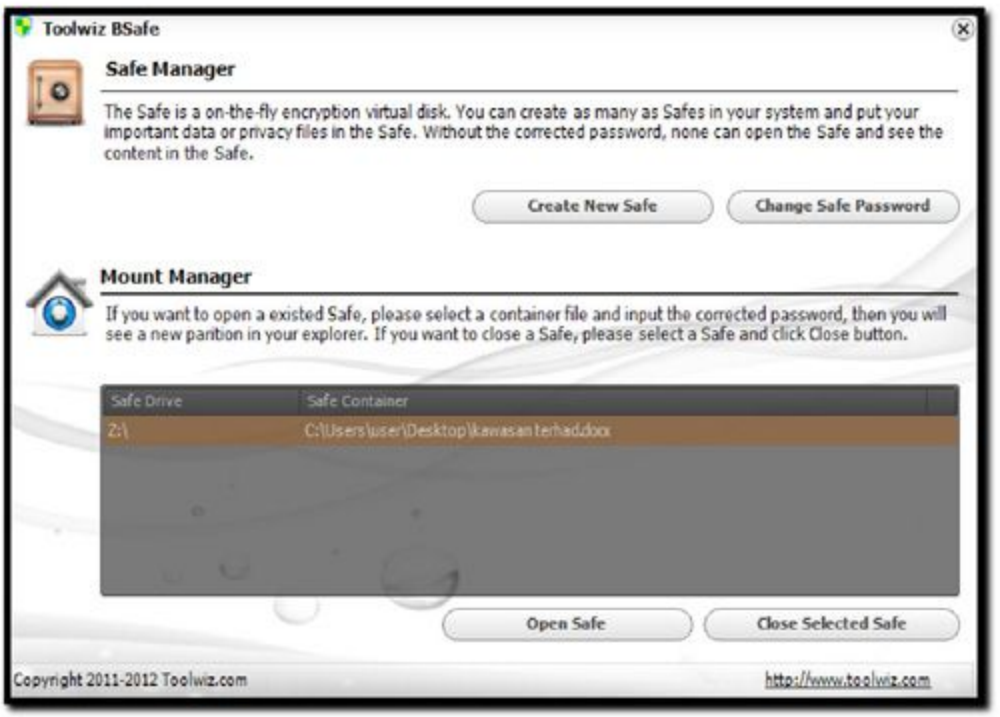
Langkah 6

Setelah selesai anda mengisi ruang kotak tersebut, kemudian tekan butang *Create Now*. Dan anda akan ditanya sama ada ingin *overwrite* dokumen tersebut atau tidak. Anda pilih *Ok*.



Langkah 7

Sila tunggu untuk proses seterusnya.

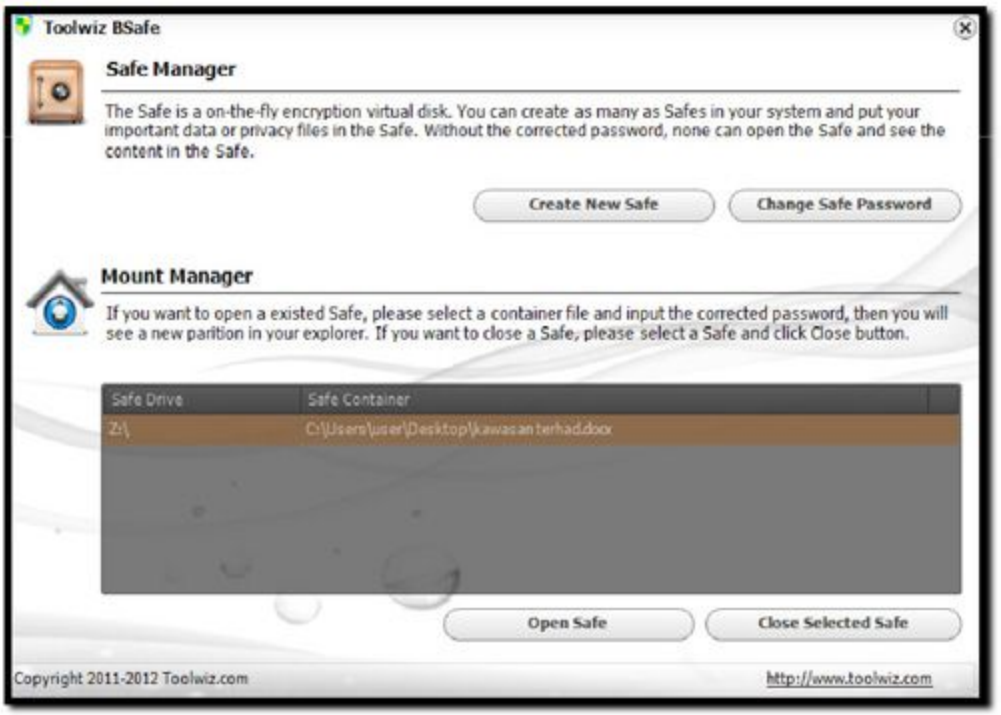


Anda akan lihat diruangan *Mount Manager* terdapat lokasi keselamatan data yang telah anda buat.

Langkah 8

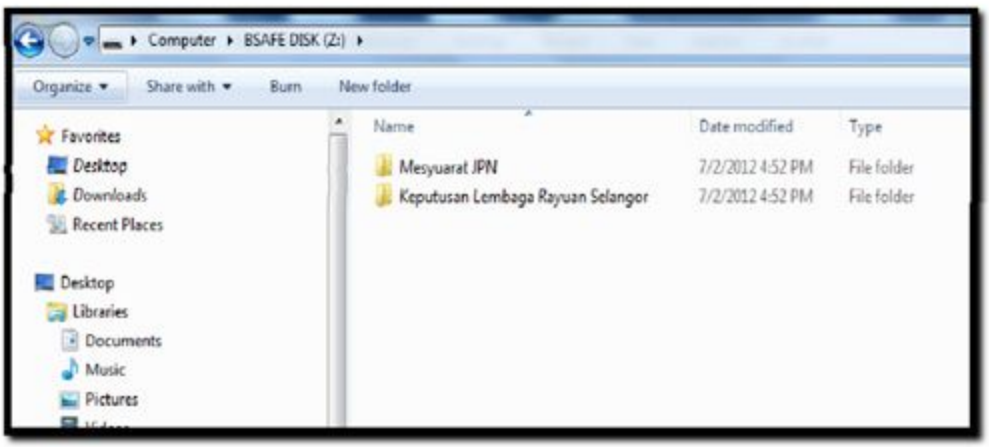
Cara penggunaan.

a) Buka perisian tersebut dan anda akan melihat diruangan *Mount Manager* terdapat lokasi keselamatan data.



b) Tekan dua kali pada pautan *Safe Drive* untuk memasuki ruangan keselamatan tersebut.
c) Paparan ini akan keluar:

d) Anda boleh membuat salinan data yang dianggap sulit kedalam ruangan ini.
e) Dibawah ini adalah contoh dokumen sulit anda.



f) Selesai.

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

JABATAN PERANCANGAN BANDAR DAN DESA NEGERI SELANGOR