GARISPANDUAN
KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)
POLITEKNIK KOTABHARU
KEMENTERIAN PENGAJIAN TINGGI MALAYSIA

Unit Sistem Teknologi Maklumat
Politeknik Kota Bharu
Kementerian Pengajian Tinggi Malaysia
KM 24, Kok Lanas
16450 Ketereh

KANDUNGAN

GARIS PANDUAN KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)
POLITEKNIK KOTA BHARU
KEMENTERIAN PENGAJIAN TINGGI MALAYSIA

1. PENGENALAN

Peningkatan penggunaan ICT dalam tugasan seharian terutama yang melibatkan Internet dan e-mel telah mendedahkan ancaman kepada pihak luar terhadap sumber ICT Politeknik Kota Bharu (PKB). Untuk memastikan maklumat-maklumat penting PKB bebas daripada ancaman, semua pengguna adalah disarankan untuk mematuhi garis panduan keselamatan ICT yang telah ditetapkan.

Garis panduan Keselamatan ICT PKB yang dikeluarkan oleh Unit Sistem Teknologi Maklumat (USTM) adalah berdasarkan garis panduan yang dikeluarkan oleh Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) dan tip dan kaedah pelaksanaan keselamatan terbaik (*best practices*) dari CyberSecurity Malaysia. Keselamatan ICT adalah meliputi semua data, peralatan ICT, perisian, rangkaian dan kemudahan ICT yang lain selaras dengan Pekeliling Am Bil. 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan dan Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

2. OBJEKTIF

Tujuan utama garis panduan keselamatan ICT PKB adalah sebagai panduan untuk menjamin kesinambungan urusan kerajaan dan menghindar kesan insiden keselamatan ICT. Keselamatan maklumat adalah untuk melindungi aset ICT PKB daripada disalahgunakan oleh

orang-orang yang tidak bertanggung jawab. Maklumat adalah berharga kerana kebanyakan informasi tersebut adalah sensitif dan terperingkat. Jika berlaku penyalahgunaan aset berkenaan kepada orang yang tidak bertanggungjawab ia bukan sahaja memudaratkan PKB malah juga kepada keselamatan dan maruah negara. Justeru itu, perlindungan keselamatan yang bijaksana perlu diwujudkan dan disesuaikan bagi menjamin kesahihan, keutuhan dan kebolehsediaan (*availability*) maklumat yang berterusan.

USTM adalah bertanggungjawab untuk melindungi maklumat terperingkat kerajaan dari dicapai oleh pengguna yang tidak sah, menjamin setiap maklumat adalah tepat dan sempurna, memastikan ketersediaan maklumat apabila diperlukan oleh pengguna dan memastikan capaian diberi hanya kepada pengguna-pengguna yang sah sahaja.

3. KESELAMATAN MAKLUMAT

3.1 Garis panduan keselamatan ICT adalah bertujuan untuk menjamin dan meningkatkan lagi tahap keselamatan maklumat yang dicapai, dihantar atau pun dirujuk. Bagi memastikan semua fail yang dihantar dan diterima bebas daripada sebarang bentuk ancaman keselamatan, perisian antivirus dan penapis *malicious codes* perlulah dikemaskini dari semasa ke semasa dan sentiasa memenuhi ciri-ciri berikut:

(a) **Kerahsiaan**

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

(b) **Integriti**

Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah oleh pegawai yang dibenarkan.

(c) **Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

(d) **Kesahihan**

Data dan maklumat hendaklah dijamin kesahihannya.

(e) **Kebolehsediaan**

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

3.2 Sekiranya penyelenggaraan komputer hendak dilaksanakan, pengguna komputer perlu memastikan semua maklumat bukan rasmi atau rahsia rasmi di dalam komputer berkenaan telah dikeluarkan dan selamat sebelum dilakukan penyelenggaraan.

4. KESELAMATAN INTERNET

Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan akses kepada banyak maklumat dalam pelbagai bentuk format dengan menyediakan penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Penggunaan Internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai tatacara yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan dan menggangu sistem dan rangkaian ICT PKB.

Demi untuk menjamin keselamatan ICT PKB pihak pengurusan telah menghadkan penggunaan Internet di mana semua pengguna mesti mencapai internet melalui *proxy server* (proksi.pkb.edu.my:8080). Pengguna Internet mestilah mematuhi prosidur dan garis panduan berikut:-

(a) Tidak dibenar melawati laman web yang tidak beretika seperti *porno* atau tidak dibenarkan (imej atau bahan-bahan yang mengandungi unsur-unsur lucah seperti *Sex, Gay, Lesbian, nude, xxx* dan seumpama dengannya).

(b) Dilarang memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik (*games*), video dan lagu.

(c) Tidak memuat turun, menyimpan dan menggunakan perisian yang tidak berlesen.

(d) Dilarang memuat turun atau naik (*download / upload*) serta menyimpan maklumat yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej organisasi atau kerajaan.

(e) Penyertaan forum atau perbincangan awam atas talian (*online forum*) mestilah mendapat kebenaran daripada Ketua Jabatan. Menggunakan kemudahan *Online chatting* atau *Internet Masseging* adalah dilarang sama sekali.

(f) Mengaktifkan *pop-up blocker tool* bagi semua penggunaan internet browser untuk menghalang *pop-up screen* yang berkemungkinan mengandungi *code / script* yang bervirus serta berunsur promosi laman web serta iklan kerana ia akan menyibukkan trafik rangkaian PKB dan internet.

(g) Dilarang memuat turun fail-fail yang saiz besar melebihi 2 MB. Sila dapatkan khidmat nasihat dari pegawai pentadbir keselamatan dan rangkaian jika ia diperlukan.

(h) Semua capaian ke Internet mestilah melalui rangkaian komputer PKB sahaja. Dilarang membuat sambungan sendiri secara dial-up kepada mana-mana ISP (JARING, TmNet, TimeNet, dan lain-lain).

5. KESELAMATAN MEL ELEKTRONIK

E-mel merupakan satu media perhubungan yang paling mudah, cepat dan murah untuk berhubung dari satu pihak dengan satu pihak yang lain tidak kira jarak, masa dan tempat. Pihak USTM juga memandang serius di dalam keselamatan perhubungan melalui e-mel di antara pegawai-pegawai PKB, terutama perhubungan dengan pihak luar yang melibatkan dokumen terperingkat. E-mel rasmi yang diperuntukkan oleh PKB sahaja (pkb.edu.my) hanya boleh digunakan untuk tujuan rasmi.

Sebagai langkah tambahan pengguna e-mel adalah dikehendaki mematuhi prosidur berikut:-

(a) **Dilarang menggunakan akaun milik orang lain**, berkongsi akaun serta membenarkan akaun digunakan oleh orang lain **walaupun** untuk tujuan **tugas rasmi**.

(b) Pengguna tidak dibenarkan dengan sewenangnya memberikan alamat e-mel PKB kepada orang lain kerana ditakuti ianya akan menggalakkan penyebaran virus, e-mel *spamming*, dan *junk-mail* seperti iklan perniagaan.

(c) Dilarang menyebarkan kod perosak seperti virus, *worm, Trojan Horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

(d) Pengguna tidak dibenarkan menggunakan e-mel untuk tujuan komersial, politik, perjudian, jenayah dan perkara-perkara lain yang mana bukan urusan rasmi jabatan.

(e) Semua e-mel yang mengandungi fail kepilan 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 akan ditapis dan ditahan penyebarannya kepada penerima kerana dikuatiri mengandungi virus.

(f) Dilarang membuka e-mel yang mengandungi fail kepilan (attachment file) seperti *.exe, *.scr, *.gif, *.pif, *.com, *.dll, *.bat, *.vbs, *.icr, *.ocx dan sebagainya yang didapati meragukan.

(g) Lakukan *scanning* ke atas semua fail dan *attachment file* bagi mengenal pasti fail-fail yang diserang virus dengan perisian antivirus yang digunakan secara rasmi oleh PKB.

(h) Memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang di alamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan.

(i) Sebarang e-mel untuk tujuan individu hendaklah dihantar terus kepada individu tersebut sahaja, dilarang menghantar e-mel kepada satu *group* seperti bahagian-bahagian tertentu. Penghantaran kepada *group* sedemikian akan mengganggu prestasi *e-mel* dan *relay server*. Dengan cara penghantaran kepada *group* juga menyukarkan bagi mengenalpasti pegawai yang perlu bertanggung jawab untuk tindakan ke atas e-mel tersebut.

(j) Untuk keselamatan **dokumen rahsia rasmi dan maklumat terperingkat tidak digalakkan dihantar melalui e-mel**, jika perlu pengguna hendaklah menggunakan **Sijil Digital** (*Digital Certificate*) untuk penghantaran dokumen tersebut melalui e-mel.

(k) Saiz fail kepilan (*attachment file*) termasuk kandungan e-mel yang dihantar hanya dibenarkan bagi saiz yang tidak melebihi **4.0 MB** sahaja. Penghantaran e-mel yang bersaiz besar akan mengganggu prestasi e-mel server dan sistem rangkaian.

(l) Pengguna yang menggunakan **Webmail PKB** hendaklah sentiasa menyelenggara e-mel supaya **saiz storan (***Inbox***)** yang digunakan untuk menyimpan e-mel tidak melebihi **20MB**, ini adalah bagi menjaga prestasi server e-mel serta prestasi capaian e-mel melalui Webmail.

(m) Pengguna e-mel perisian **outlook** hendaklah **sentiasa menyelenggara e-mel** supaya saiz setiap *folder* terutama *folder* INBOX tidak melebihi **500MB**, ini adalah bagi menjamin prestasi perisian e-mel *outlook* dan komputer pengguna.

(n) Pengguna hendaklah **mencetak e-mel yang penting** dan **difailkan** bagi **mengelak maklumat penting hilang** apabila berlaku kerosakan kepada *hard disk* komputer atau serangan virus.

(o) Pengguna hendaklah membuat salinan dan **menyimpan** *attachment file* **ke satu** *folder* **berasingan** dari e-mel-e-mel yang penting bagi tujuan *backup* jika berlaku masalah kepada *hard disk* komputer.

(p) Pihak **USTM tidak akan bertanggung jawab** ke atas **e-mel yang hilang** bagi pengguna yang tidak mematuhi polisi penggunaan e-mel.

(q) Alamat e-mel rasmi PKB hanyalah untuk kegunaan menghantar e-mel yang rasmi atau tugasan pejabat, sebarang e-mel yang tidak ada kaitan dengan tugasan pejabat adalah dilarang.

(r) Penggunaan alamat e-mel yang tidak rasmi seperti *yahoo.com, hotmail.com, gmail.com* atau sebagainya adalah dilarang untuk tugas-tugas rasmi, sama ada untuk urusan dalaman atau luaran PKB.

(s) Dilarang membuat penyebaran/*forward* e-mel yang tidak rasmi menggunakan alamat e-mel PKB.

6. KESELAMATAN RANGKAIAN

6.1 Rangkaian adalah merupakan satu sumber ICT yang utama bagi sesebuah organisasi pada masa kini. Oleh itu, keselamatan rangkaian (*network security*) adalah merupakan satu langkah keselamatan utama untuk mengawal aset ICT dari dicerobohi. Rekabentuk rangkaian yang betul dan baik adalah merupakan satu faktor keselamatan rangkaian komputer sesebuah organisasi. Untuk menjamin keselamatan rangkaian di PKB, pihak USTM telah membangunkan satu rekabentuk rangkaian yang tersusun dan sentiasa dikemas kini dan mengutamakan keselamatan.

6.2 Pemantauan juga dilakukan dari masa ke semasa untuk memastikan keselamatan rangkaian dan server PKB di setiap *zone* sentiasa berada di dalam keadaan baik. Pengguna tidak dibenarkan memuat turun apa juga perisian seperti *screen saver*, *games*, gambar dan perkara-perkara yang seperti dengannya kerana ia akan memberi impak kepada prestasi rangkaian (*network performance*) dan kemungkinan ada virus atau kod virus bersamanya.

6.3 *Firewall* diwujudkan bagi memastikan keselamatan ke atas aset-aset di dalam rangkaian PKB supaya tidak diceroboh oleh orang yang tidak bertanggung jawab. Melalui sistem *Firewall* tersebut hanya server-server dan perkhidmatan *port* tertentu sahaja yang

dibenarkan kepada pengguna dari luar untuk mencapai server-server dalaman. Konfigurasi keselamatan Setiap server diperkemaskan dan dikemaskini dari semasa ke semasa selain dari kawalan capaian oleh *firewall*.

6.4 Selain dari menyediakan infrastruktur rangkaian yang baik, USTM juga sentiasa memantau setiap log di dalam setiap server untuk memastikan tidak ada capaian yang tidak sah dibuat ke atas server berkenaan.

6.5 *Firewall, Proxy* atau *webcache server, IPS, anti spamming* dan *viruswall server* juga diwujudkan bagi mengawal serta memantau penggunaan internet. Ia berfungsi mengawal pengguna dari melayari laman web *prono* atau lucah serta mengawal pengguna dari memuat turun fail-fail tertentu seperti gambar lucah, lagu, video dan sebagainya.

7. KESELAMATAN KATALALUAN (*PASSWORD*)

Katalaluan adalah merupakan kunci atau *pin* yang menjadi hak individu, ia perlu dirahsiakan dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga katalaluan masing-masing dengan teliti dari dicuri dan disalahguna oleh pengguna lain. Bagi menjamin keselamatan Katalaluan pengguna perlulah mematuhi prosidur berikut:-

(a) Sekiranya katalaluan telah dicuri atau disyaki dicuri, laporan hendaklah dibuat kepada pentadbir sistem ICT dan kata laluan sedia ada hendaklah diubah dengan serta merta.

(b) Katalaluan perlu ditukar sekerap mungkin dan dacadangkan sekurang-kurangnya sebulan sekali.

(c) Panjang Kataluan hendaklah mempunyai sekurang-kurangnya lapan (8) aksara dengan gabungan *alphanumeric* huruf kecil dan besar serta simbol khas.

(d) Katalaluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media terutama menulisnya disebelah monitor.

(e) Sila lawati *http://email.pkb.gov.my/* untuk mengetahui cara-cara untuk mengubah password e-mel dan cara-cara untuk mengaktifkan *password* komputer anda seperti di LAMPIRAN A.

8. KESELAMATAN KOMPUTER DAN *NOTEBOOK* SERTA PERALATAN

Keselamatan meliputi komputer, *notebook* dan perkakasan terlibat seperti *hard disk*, pencetak, pengimbas dan lain-lain. Pengguna seharusnya memastikan komputer atau *notebook* dan peralatan yang digunakan sentiasa mematuhi garis panduan berikut:

(a) Setiap komputer atau *notebook* mestilah mempunyai katalaluan.

(b) Komputer atau *notebook* perlulah dilakukan pengemaskinian *Microsoft Windows, patches* dan *services pack* yang terkini.

(c) Setiap komputer atau *notebook* perlulah ada *computer name* yang sesuai dengan pemilik. *Joint Domain* PKB dan perisian *antivirus*.

(d) Pastikan antivirus sentiasa dikemaskini supaya dapat menangani serangan virus yang baru.

(e) Dilarang membuat instalasi perisian yang tidak berlesen atau perisian yang tidak rasmi penggunaannya di PKB ke dalam komputer atau *notebook*.

(f) Dilarang membuat instalasi perisian *screen server* atau *active desktop* kerana akan menyebabkan prestasi komputer menjadi perlahan.

~~(g) Semua komputer hendaklah menggunakan *wallpaper desktop* korporat PKB.~~

(h) Dilarang mengubah atau meminda *computer name* dan *description* dalam komputer.

(i) Pastikan komputer atau *notebook* pejabat tidak digunakan oleh orang yang tidak berkenaan.

(j) Pastikan komputer atau *notebook* diletakkan di tempat dingin dan kering serta selamat persekitarannya.

(k) Dilarang menggunakan alat penyambung kuasa elektrik bagi berbagai peralatan. Bekalan kuasa elektrik yang tidak stabil akan merosakkan komputer. Gunakan kemudahan *Uninterruptable Power Supply* (UPS) atau *Automatic Voltage Regulator* (AVR) untuk memastikan bekalan elektrik sentiasa dibekalkan mengikut spesifikasi keperluan komputer/*notebook*.

(l) Pastikan bekalan atau punca elektrik ditutup semasa pemasangan atau penyambungan peralatan komputer dan aksesorinya atau setelah selesai menggunakan komputer atau *notebook.*

(m) Pastikan komputer atau *notebook* tidak terdedah secara terus kepada pancaran matahari/haba dan elakkan komputer daripada kawasan tarikan kuasa magnet/kuasa voltan yang tinggi.

(n) Rehatkan komputer atau *notebook* jika terlalu kerap menggunakan secara berterusan.

(o) Tamatkan proses *not responding* dengan kekunci *Ctrl-Alt-Del* jika PC *hang*. Tidak digalakkan menutup suis sekiranya PC menjadi *hang.*

(p) Tidak digalakkan membuka program yang banyak secara serentak di dalam sistem komputer atau *notebook* bagi mengelakkan sistem menjadi *hang*.

(q) Pastikan komputer atau *notebook* mempunyai *system date & time* yang betul untuk tujuan audit dan penghantaran e-mel.

(r) Sentiasa matikan komputer dengan cara yang betul bagi mencegah kerosakan kepada *operating system* (OS) *Windows*.

(s) Dilarang menghentak/mengetuk dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer atau *notebook*.

(t) *Notebook* yang digunakan atau dibawa ke luar pejabat hendaklah sentiasa dikunci dengan tali pengunci *notebook* sama ada semasa berkerja di meja mahupun di dalam kereta perlu dikunci pada kerusi atau sebagainya.

(u) Tidak dibenarkan membaiki sendiri komputer atau *notebook* jika ada masalah atau kerosakan.

(v) USTM berhak untuk menghapus fail-fail atau maklumat-maklumat yang tidak ada kaitan dengan tugas rasmi seperti fail lagu dan gambar membuang program-program yang tidak ada kaitan dengan tugas rasmi.

9. KESELAMATAN TATACARA PENJAGAAN MEDIA STORAN

Media storan yang popular digunakan pada masa sekarang adalah USB *Drive*. Walaubagaimana pun Disket atau cakera liut masih lagi digunakan oleh sesetengah pengguna sebagai media storan elektronik untuk menyimpan data atau fail yang kecil untuk penyebaran maklumat atau sebagai *backup*. Bagi memastikan data yang disimpan sentiasa selamat oleh itu pengguna dinasihatkan supaya mengikut prosidur tatacara penjagaan media storan seperti berikut:-

(a) Elakkan disket dari terkena debu-debu atau habuk dan hendaklah disimpan di tempat yang selamat.

(b) Sekiranya disket yang digunakan adalah yang telah lama jangkahayatnya, maka data atau fail hendaklah dipindahkan ke media lain yang lebih tahan lama dan selamat seperti CD/DVD.

(c) Media storan yang rosak atau tidak boleh digunakan lagi, perlulah dimusnahkan sebelum dibuang. Ini adalah bagi mempastikan maklumat di dalamnya betul-betul tidak dapat dicapai oleh orang lain.

(d) CD/DVD hendaklah disimpan di tempat yang selamat agar ia tidak tercalar dan rosak.

(e) Semua media stroran hendaklah tidak disimpan berhampiran dengan sumber-sumber yang bermagnet, bagi mengelakkan data yang disimpan hilang atau rosak.

(f) Semua media storan seperti disket, *CD, DVD* dan *Handy Drive* hendaklah dibuat pemeriksaan virus terlebih dahulu sebelum digunakan. Pemeriksaan virus tersebut hendaklah dibuat secara berkala bagi menjamin keselamatan data atau maklumat yang disimpan.

10. KESELAMATAN KOMPUTER DI BILIK SEVER

Sebahagian besar server-server aplikasi PKB ditempatkan di bilik server untuk tujuan pengurusan server secara berpusat. Semua data-data yang disimpan di dalam server adalah aset yang penting dan perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dilaksanakan bagi melindungi server-server tersebut seperti berikut:-

(a) Setiap server perlu dilabelkan untuk memudahkan setiap pentadbir menjalankan tugas masing-masing.

(b) Pengguna perlu mencatat buku log yang disediakan sebelum memasuki bilik server.

(c) Pastikan bilik server sentiasa bersih supaya server serta peralatan-peralatan yang di tempatkan k\dan komputer tidak terdedah kepada habuk.

(d) Penghawa dingin mestilah berfungsi dengan baik dimana suhunya berada dalam lingkungan ±19.5°C dan kelembapan di paras 50.7%. Dan ia perlu dipantau agar tidak berlaku kebocoran yang boleh merosakkan peralatan-peralatan dibilik server.

(e) Kertas-kertas cetakan yang tidak digunakan perlulah dis*hred*/diricih.

11. KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA

Data dan maklumat sistem aplikasi PKB yang telah dibangunkan dan beroperasi merupakan aset yang penting dan perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dikenalpasti dan dilaksanakan bagi melindungi aset-aset tersebut seperti berikut:-

11.1 **Pembaikpulih Sistem**

Pembaikpulih Sistem adalah merupakan proses baikpulih akibat dari kemusnahan atau kehilangan data yang berlaku atas banyak sebab di antaranya adalah :-

- kegagalan server berfungsi
- kerosakan fizikal *hard disk*
- masalah kesilapan dalam pemprograman
- kesan pencerobohan
- kesan bencana alam

Proses pembaikpulih sistem terbahagi kepada dua peringkat iaitu **prosidur backup** dan **prosidur baikpulih.**

11.1.1 **Prosidur Backup**

(a) *Backup* kepada keseluruhan server semua data dan aplikasi termasuk *Operating System* (OS) dibuat pada setiap malam untuk semua server. Beberapa prosidur *backup* dilakukan ke atas semua data-data yang disimpan di dalam server.

Kekerapan penjanaan data *backup* adalah mengikut kepentingan data-data tersebut secara berperingkat dari harian hinggalah bulanan.

Selain backup terhadap data-data, terdapat juga backup yang dilakukan kepada transaksi selepas backup sehingga ke transaksi paling akhir diproses sebelum kerosakan berlaku.

Menjana backup ini dipanggil *backup logical log*.

(b) *Backup* atau salinan data ke dalam pita atau media lain perlu dilakukan setiap hari untuk mengelakkan kehilangan data sekiranya berlaku kerosakan *hard disk.*

(c) Labelkan setiap media storan *backup* yang digunakan bagi memudahkan proses baikpulih dilaksanakan.

(d) *Backup* sistem aplikasi dan sistem operasi perlu diadakan sekurang-kurangnya sekali bagi setiap keluaran versi terbaharu 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*.

(e) *Backup* untuk data dan sistem aplikasi/sistem operasi 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 Bahagian Teknologi Maklumat
- Lokasi *off-site* kedua – di bangunan lain yang berdekatan atau mana-mana Jabatan Kerajaan lain yang berdekatan dan mempunyai kemudahan untuk menyimpan media *backup*.

(f) Penetapan lokasi simpanan backup ini adalah untuk memastikan data-data kritikal/penting masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebagainya.

11.1.2 **Prosidur Baikpulih**

Dengan prosidur *backup* di atas, proses membaikpulih boleh dilakukan sama ada dari peringkat paling kritikal seperti kegagalan seluruh *partition hardisk* atau pangkalan data *(database*), aplikasi, direktori sehingga ke atas fail tertentu dapat dibaikpulih dengan mudah dan selamat.

11.2 Pelan Pemulihan Bencana

Data-data kritikal di*backup* ke dalam pita (*tape*) dan disimpan di bilik server, disamping itu pendua bagi data-data tersebut dihantar dan disimpan di agensi lain sebagai salah satu pelan pemulihan bencana. Amalan ini dilakukan bagi memastikan data-data kritikal masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal di bilik server, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebaginya.

12. KESELAMATAN DARI ANCAMAN VIRUS

Serangan virus komputer merupakan masalah yang sentiasa dihadapi oleh PKB dan dilain-lain organisasi lain yang menggunakan komputer. Kepelbagaian jenis virus akan menyebabkan kerosakan sistem pengoperasian serta peralatan komputer lain seperti *hard disk*. Ia juga menyebabkan maklumat atau data penting menjadi rosak atau hilang dan

mungkin juga ia disebar kepada orang-orang berkenaan tanpa pengetahuan pengguna.

Sebagai langkah keselamatan USTM juga telah membuat tapisan di server *antispamming* untuk mengawal penyebaran virus melalui e-mel. Server akan menapis sebarang e-mel yang mempunyai fail *.exe, *.scr, *.gif, *.pif, *.com, *.dll, *.bat, *.vbs, *.icr dan *.ocx. Kesemua fail berkenaan adalah berkemungkinan besar pembawa virus.

Untuk meningkatkan lagi tahap keselamatan PKB semua pengguna dikehendaki mengambil langkah-langkah berikut :-

(a) Pengguna PC mestilah sentiasa melakukan nyah virus (*virus scan*) di PC dan semua media storan yang digunakan untuk mempastikan tidak ada virus sebelum ia digunakan. Dengan itu kita dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus.

(b) Sekiranya terdapat serangan virus ke atas data atau dokumen dan jika virus tersebut tidak dapat dihapuskan, sila hubungi pihak USTM untuk bantuan teknikal.

(c) Media storan seperti Disket, *handy drive, CD* atau DVD dan lain-lain yang diperolehi dari luar perlulah di*scan* atau dinyah virus terlebih dahulu sebelum digunakan. Dilarang membuka data atau dokumen yang virus yang tidak dapat dihapuskan. Sila dapatkan khidmat nasihat teknikal daripada USTM

(d) Semua fail hendaklah di *scan* dengan anti virus terlebih dahulu sebelum ia disimpan atau disalin ke *Storage Server*.

(e) Semua *notebook* atau komputer PC dari luar hendaklah di*scan virus* terlebih dahulu sebelum ia disambung ke sistem rangkaian PKB.

Sekiranya terdapat ia mengandungi virus dan tidak dapat dihapuskan sila hubungi USTM untuk bantuan teknikal.

13. KHIDMAT NASIHAT

Sebarang kemusykilan atau pertanyaan berkaitan Garis Panduan Mengenai Keselamatan ini sila hubungi Unit Rangkaian & Keselamatan ICT, Unit Sistem Teknologi Maklumat.

Tn. Haji Azahan Bin Haji Daud : Sambungan 141
(azahanhd@pkb.edu.my)

Pn. Suzianna Binti Taib : Sambungan 225
(suzianna@pkb.edu.my)

14. PENUTUP

Secara ringkasnya keselamatan ICT PKB ini perlu dilaksanakan secara menyeluruh, sekiranya salah satu individu, unit, seksyen atau bahagian yang tidak melaksanakannya ia akan menjejaskan keselamatan keseluruhan PKB. Oleh itu, keselamatan ICT merupakan tanggungjawab semua pihak dan ia tidak hanya dikhususkan kepada satu pihak sahaja. Garispanduan keselamatan ini juga akan dikemaskini dari semasa ke semasa tertakluk kepada keperluan keselamatan ICT dan arus perubahan global ICT.

Langkah-langkah menukar password.

- kena buat step tukar password melalui domain.