GARIS PANDUAN KESELAMATAN ICT

JABATAN KEHAKIMAN SYARIAH MALAYSIA (JKSM)
VERSI 1.0

BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (BTMK)

JABATAN KEHAKIMAN SYARIAH MALAYSIA (JKSM)

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
20 Disember 2016	**1.0**	**Mesyuarat Jawatankuasa Keselamatan ICT Bil.2/2016**	**20 Disember 2016**

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN	MUKA SURAT

ISI KANDUNGAN

TATACARA PENGGUNAAN DAN KESELAMATAN ICT
JABATAN KEHAKIMAN SYARIAH MALAYSIA

1.0 TATACARA PENGGUNAAN INTERNET

Berikut adalah tatacara penggunaan Internet yang mesti dipatuhi dan diikuti dalam menggunakan Internet.

1.1.1 Hak Terhadap Capaian Oleh Pengguna

Ianya boleh dilihat sebagai satu kemudahan yang disediakan oleh JKSM untuk memudahkan dan melicinkan semua urusan rasmi yang melibatkan aset ICT. Semua pengguna harus maklum bahawa semua aset ICT termasuk maklumat yang diperolehi adalah aset kerajaan.

1.1.2 Pemilihan Laman Yang Hendak Dilayar

Pengguna hanya dibenarkan melayari laman yang berkaitan dengan urusan rasmi kerja dan laman yang mendapat kebenaran khas dari Ketua Jabatan.

1.1.3 Pengesahan Maklumat

Semua bahan dan sumber maklumat yang diperolehi dari Internet hendaklah disahkan ketepatan dan kesahihan. Menyatakan sumber rujukan maklumat yang diperolehi dari Internet amatlah digalakkan.

1.1.4 Muat Naik Bahan

Bahan rasmi yang hendak dimuat naik mestilah mendapat pengesahan dan kebenaran daripada Ketua Jabatan sebelum dimuat naik.

1.1.5 Muat Turun Bahan

Semua bahan yang hendak dimuat turun hendaklah dipastikan sah seperti perisian yang berdaftar dan di bawah Hak Cipta Terpelihara. Semua bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan sahaja.

1.1.6 Perbincangan atau Forum Awam

Hanya warga JKSM/JKSN/MSN yang mendapat kebenaran sahaja boleh menggunakan kemudahan ini. Namun begitu, semua maklumat dan kandungan bagi forum awam ini perlulah mendapat kebenaran rasmi dari Ketua Jabatan. Ini kerana semua maklumat yang hendak dikongsi akan melambangkan imej dan nama baik JKSM/JKSN/MSN.

1.2 Larangan Dan Salah Laku Pengguna Internet

Pengguna Internet adalah dilarang sama sekali melakukan perkara yang berikut:

1.2.1 Melayari laman web yang tidak beretika seperti porno atau laman web yang tidak dibenarkan atau bahan- bahan yang mengandungi unsur-unsur lucah;

1.2.2 Memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;

1.2.3 Memuat turun, menyimpan dan menggunakan perisian yang tidak tulen;

1.2.4 Memuat turun, memuat naik dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan individu atau kerajaan;

1.2.5 Menyertai forum atau perbincangan awam atas talian (*online forum*) tanpa kebenaran daripada Ketua Jabatan;

1.2.6 Pengguna Internet digalakkan untuk mengaktifkan *popup blocker tool* bagi setiap Internet *browser* yang digunakan untuk mengelakkan paparan imej-imej yang tidak dikehendaki. Sebagai contoh *Yahoo Toolbar* dan *Google Toolbar*;

1.2.7 Memuat turun fail-fail yang bersaiz besar sehingga 10 MB. Bagi saiz fail melebihi 10 MB ianya hendaklah mendapatkan khidmat nasihat dari Pentadbir Sistem Emel terlebih dahulu;

1.2.8 Pengguna yang menggunakan aplikasi web adalah bertanggungjawab sepenuhnya ke atas maklumat yang di *key-in;*

1.2.9 Menceroboh atau percubaan untuk menggodam laman web JKSM/JKSN/MSN;

1.2.10 Mendengar radio secara*online* kerana ia boleh mengganggu prestasi rangkaian JKSM/JKSN/MSN;

1.2.11 Membuat capaian terus ke Internet atau mana-mana rangkaian luar dengan menggunakan modem atau perkakasan lain di dalam persekitaran rangkaian JKSM/JKSN/MSN tanpa kebenaran dari Pentadbir Rangkaian (seperti Jalur lebar *(broadband)*);

1.2.12 Menggunakan kemudahan Internet untuk tujuan peribadi;

1.2.13 Menjalankan aktiviti-aktiviti berunsur komersial dan politik;

1.2.14 Menggunakan kemudahan *chatting* melalui Internet (seperti *Yahoo Messenger* dan *gtalk*);

1.2.15 Melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas;

1.2.16 Mengubah apa-apa juga konfigurasi terhadap rangkaian bagi niat untuk mendapatkan akses terhadap Internet tanpa kebenaran dari Ketua Jabatan;

1.2.17 Menyedia, memuat naik, memuat turun, menyimpan dan menyebar material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur ganas dan berbaur perkauman;

1.2.18 Memuat naik, memuat turun, menyimpan dan menyebar gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;

1.2.19 Menggunakan *proxy* lain selain dari yang telah ditetapkan oleh Pentadbir Rangkaian; dan

1.2.20 Membuat cubaan berulang-ulang terhadap laman web yang telah disekat.

2.0 TATACARA PENGGUNAAN EMEL

2.1 Terdapat dua kategori emel rasmi:

2.1.1 Emel rahsia rasmi

Mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada *Terhad, Sulit, Rahsia* atau *Rahsia Besar.*

2.1.2 Emel bukan rahsia rasmi

Tidak mengandungi maklumat atau perkara rahsia rasmi.

2.2 Kaedah pengendalian dan penggunaan emel adalah seperti yang berikut:

2.2.1 Pemilikan Akaun Emel

Penggunaan akaun milik individu lain atau berkongsi akaun adalah dilarang. Kemudahan emel ini juga bukan merupakan hak mutlak individu dan perlu ditarik balik sekiranya individu bertukar keluar, berhenti atau berpencen dari JKSM/JKSN/MSN.

2.2.2 Format Emel

Penghantar emel hendaklah memastikan bahawa kandungan emel adalah bersesuaian dan berkaitan

dengan perkara yang dibincangkan sebelum penghantaran dibuat.

Penggunaan huruf besar di dalam emel adalah tidak digalakkan dan dianggap tidak beretika. Gabungan huruf besar dan kecil boleh digunakan di tempat- tempat tertentu yang difikirkan bersesuaian di samping mengamalkan penggunaan bahasa yang betul, ringkas dan sopan.

Setiap emel rasmi hendaklah disertakan dengan tandatangan emel *(email signature)* yang mengandungi maklumat asas pengirim seperti nama penuh, jawatan, jabatan, bahagian, unit, alamat pejabat, nombor telefon, nombor faksimili dan alamat emel. Maklumat ini adalah penting untuk dihubungi dan mencerminkan imej JKSM.

2.2.3 Penghantaran Emel

Akaun emel rasmi hendaklah digunakan bagi tujuan penghantaran emel rasmi dan pastikan dihantar ke alamat emel yang betul. Penggunaan ‘salinan kepada’ (*cc*) adalah dibenarkan sekiranya emel tersebut perlu dimaklumkan kepada penerima lain. Walaubagaimanapun, penggunaan *’blind cc’* adalah tidak digalakkan.

Kemudahan balas (*re*ply) digunakan untuk menjawab emel kepada penghantar asal dan panjangkan *(forward)* untuk memanjangkan emel atau dimajukan kepada penerima lain.

Setiap emel rasmi yang diterima hendaklah dijawab dengan cepat dan diambil tindakan dengan segera apabila emel berkenaan diterima.

Penggunaan kemudahan emel jawab automatik hendaklah diaktifkan bagi pengguna yang akan berada di luar pejabat dan dinyahaktifkan selepas kembali ke pejabat.

2.2.4 Penghantaran Bersama Fail Kepilan

Saiz fail kepilan *(attachment file)* termasuk kandungan emel yang dibenarkan untuk penghantaran adalah tidak melebihi 10 MB sahaja.

Ini adalah arahan selaras dengan surat yang dikeluarkan oleh MAMPU bertajuk “Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan” rujukan UPTM159/526/9 Jld.4 (60) yang bertarikh 23 November 2007 dan “Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan” rujukan UPTM159/526/9 Jld.4(59) bertarikh 1 Jun 2007 yang berkaitan.

2.2.5 Mengenal Pasti Identiti Pengguna

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

2.2.6 Saiz Storan Penyimpanan

Saiz storan yang dibekalkan adalah mengikut jawatan seperti berikut :

(a) Ketua Hakim – tiada had (*unlimited*)
(b) Ketua Pendaftar – 500MB
(c) Pengarah/ Pengarah Kanan – 500MB
(d) Lain-lain jawatan – 200MB

Pengguna adalah dinasihatkan supaya melakukan penyelenggaraan agar saiz storan untuk menyimpan emel tidak melebihi 75% daripada saiz storan yang diberikan.

2.2.7 Pemusnahan dan Penghapusan

Emel yang tidak diperlukan dan tidak mempunyai nilai arkib yang telah diambil tindakan hendaklah dihapuskan (Contoh: draf kertas kerja, draf minit dan kertas makluman).

2.2.8 Pemeriksaan oleh Pentadbir Emel JKSM

Pentadbir emel JKSM berhak untuk memantau emel pengguna sekiranya perlu tanpa mendapatkan kebenaran dari pengguna.

2.2.9 Penggunaan Kata Laluan

Pengguna hendaklah mengikut tatacara kata laluan yang telah ditetapkan seperti yang dinyatakan dalam perkara 6.0.

2.3 Larangan dan Salahlaku Pengguna Emel

Pengguna emel adalah dilarang sama sekali melakukan perkara yang berikut:

i. Menggunakan akaun emel milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

ii. Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;

iii. Menggunakan emel untuk tujuan komersial atau politik.

iv. Membuka emel dari penghantar yang tidak dikenali dikhuatiri mengandungi virus;

v. Membalas emel yang diterima daripada sumber yang tidak diketahui dan diragui;

vi. Menyebarkan kod perosak seperti virus, *worm, Trojan Horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

vii. Membuka emel 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 yang berkemungkinan akan menyebarkan virus apabila dibuka;

viii. Menghantar, memiliki dan menyimpan bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;

ix. Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi JKSM dan Perkhidmatan Awam

melalui kemudahan emel JKSM. Pihak JKSM tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan emel;

x. Menghantar dan melibatkan diri dalam emel yang berunsur emel sampah (*junk*), emel bom, emel *spam*, emel berantai, fitnah, ciplak dan aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Malaysia;

xi. Menghantar semula emel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian;

xii. Membenarkan pihak ketiga untuk menjawab emel kepada penghantar asal bagi pihaknya; dan

xiii. Menyedia atau menghantar maklumat berulang-ulang yang berupa gangguan.

2.4 Tanggungjawab dan Peranan Pengguna Emel

Peranan dan tanggungjawab pengguna adalah seperti berikut :

i. Mencetak dan mendokumenkan semua emel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada pelayan;

ii. Membuat salinan dan menyimpan fail kepilan ke satu *folder* berasingan dari setiap emel yang penting bagi tujuan salinan (*backup)*;

iii. Melakukan imbasan ke atas semua fail yang akan dihantar dan fail kepilan yang diterima bagi memastikan fail-fail tersebut bebas daripada serangan virus;

iv. Memaklumkan kepada pentadbir emel sekiranya hendak bertukar keluar Jabatan, berhenti dan bersara dari Jabatan

selewat-lewatnya tiga (3) hari sebelum tarikh akhir perkhidmatan;

v. Memaklumkan kepada Pentadbir Emel dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

vi. Bertanggungjawab sepenuhnya terhadap semua kandungan di dalam akaun emel sendiri;

vii. Menggunakan kemudahan emel jawab automatik setiap kali berada di luar pejabat atau bercuti dan dinyahaktifkan semula emel jawab automatik setelah kembali ke pejabat; dan

viii. Menggunakan kemudahan *forwarding* bagi pegawai yang akan meninggalkan pejabat bagi memastikan tindakan ke atas emel dapat diambil dengan kadar segera.

2.5 Tanggungjawab Pentadbir Emel

Bagi memastikan pengendalian emel JKSM beroperasi dengan lebih efisyen dan berkesan, Pentadbir Emel adalah bertanggungawab:

2.5.1 Memastikan setiap akaun emel yang diwujudkan atau dibatalkan telah mendapat kelulusan dari Ketua Jabatan tempat bertugas pemohon menggunakan Sistem Borang *On-Line* (http://jksm.esyariah.gov.my). Pembatalan akaun (pengguna yang berhenti, bertukar dan yang melanggar dasar dan tatacara penggunaan emel JKSM) perlulah dilakukan dengan segera bagi memastikan keselamatan maklumat;

2.5.2 Menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan emel pengguna yang lemah dan kemudiannya mencadang dan memperakukan ciri-ciri kata laluan yang lebih baik kepada

pengguna. Aktiviti ini perlu dibuat sekurang-kurangnya tiga (3) kali setahun;

2.5.3 Menjalankan pemantauan dan penapisan kandungan fail elektronik dan emel secara berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna. Ini bertujuan memastikan pelaksanaannya mematuhi dasar dan tatacara yang ditetapkan;

2.5.4 Memastikan sistem emel beroperasi dengan baik dan boleh dicapai sepanjang masa (24 X 7 X 365);

2.5.5 Akaun emel yang didapati tidak aktif untuk tempoh selama tiga (3) bulan, Pentadbir Emel berkuasa untuk menyahaktifkan sementara (*disable)* akaun emel tersebut tanpa notis. Jika tiada aduan diterima dalam tempoh tiga puluh (30) hari, Pentadbir Emel berkuasa untuk menghapuskan (*delete*) akaun tersebut;

2.5.6 Akaun emel bagi individu yang akan bersara, bertukar keluar dari Jabatan atau yang dikenakan tindakan tatatertib akan dihapuskan dalam tempoh tiga puluh (30) hari. Ianya bertujuan untuk memastikan semua akaun emel tersebut diuruskan dengan lebih efektif dan efisyen bagi memastikan tidak berlaku kehilangan dan kebocoran maklumat yang penting dari emel tersebut;

2.5.7 Pemakaian Prosedur ini merangkumi semua pegawai dan kakitangan yang akan bertukar keluar Jabatan, berhenti dan berpencen seperti yang berikut:

a. Bertukar keluar dari JKSM/JKSN/MSN;

b. Bersara wajib atau pilihan;

c. Kemudahan penggunaan emel ditarik balik atas sebab tertentu;

d. Bercuti untuk meneruskan pengajian (tidak ditugaskan semula ke JKSM/JKSN/MSN);

e. Mengikuti program anjuran agensi kerajaan (tidak ditugaskan semula ke JKSM/JKSN/MSN); dan

f. Ditamatkan perkhidmatan

2.5.8 Tatacara pemberian ID akaun emel.

Pengwujudan ID bagi akaun emel hendaklah mengikut garis panduan seperti yang ditetapkan seperti yang berikut:

2.5.8.1 ID bagi akaun emel pengguna hendaklah menggunakan nama sebenar. Penggunaan nama samaran atau gelaran tidak dibenarkan.

Contoh:

ghalif@esyariah.gov.my = betul

ghalif_happy@esyariah.gov.my = salah

2.5.8.2 Bagi ID baru yang mempunyai persamaan dengan yang sedia ada. Maka penggunaan pangkal huruf bagi nama bapa hendaklah digunakan seperti berikut:

Contoh:

Razak Bin Ahmad = razak.a@esyariah.gov.my

2.5.9 Memberi latihan tatacara pengendalian dan pengurusan emel kepada pegawai sekiranya perlu;

2.5.10 Program kesedaran tatacara dan pembudayaan penggunaan emel juga perlu dilaksanakan secara berkala bagi menjamin keberkesanan sistem emel;

2.5.11 Memantau kestabilan server *(server health)* 24 x 7 x 365 dengan menguji capaian kepada sistem emel secara berkala dengan menggunakan peralatan yang dikenal pasti sesuai;

2.5.12 Memastikan *Standard Operating Procedures (SOP)* disediakan berdasarkan kepada garis panduan yang disediakan oleh MAMPU;

2.5.13 Membuat salinan pendua atau *backup* emel pada setiap hari;

2.5.14 Memastikan *Business Continuity Plan* (BCP) dan *Risk Assessment* disediakan bagi sistem emel di JKSM; dan

2.5.15 Mengadakan sesi perbincangan dengan pembekal-pembekal utama sistem emel dari semasa ke semasa untuk mencari jalan terbaik bagi memperbaiki pengurusan dan pengoperasian sistem emel secara berterusan.

2.6 Kelayakan

Kelayakan kemudahan emel ini diberikan kepada kakitangan JKSM yang menjalankan urusan komunikasi dan perhubungan elektronik secara rasmi.

3.0 KAWALAN KESELAMATAN EMEL DAN INTERNET

3.1 Keselamatan Fizikal

Semua perkakasan yang mempunyai capaian terhadap emel dan Internet JKSM seperti komputer peribadi, komputer riba atau komputer *tablet* hendaklah diletak atau disimpan di tempat yang mempunyai kawalan dari pencerobohan.

3.2 Keselamatan Dokumen Elektronik

Semua maklumat rahsia rasmi atas talian perlu berada dalam bentuk teks sifer sepanjang masa, manakala maklumat rahsia rasmi yang tidak diperlukan atas talian mesti dipindahkan segera ke media storan elektronik sekunder dalam bentuk teks sifer dan hendaklah dikelaskan. Peraturan mengelaskan maklumat digital telah digariskan dalam dokumen *Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS), Buku Arahan Keselamatan dan Surat Pekeliling Am Bil. 2 Tahun 1987 "Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986".

3.3 Tandatangan Digital

Bagi mengendalikan maklumat rahsia rasmi, JKSM mesti menggunakan tandatangan digital yang dikeluarkan oleh pihak berkuasa perakuan tempatan yang ditauliahkan oleh Kerajaan Malaysia iaitu Pihak Berkuasa Persijilan *(Certification Authority).*

3.4 Keselamatan Pengendalian Emel Rahsia Rasmi

Perkara–perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan emel rahsia rasmi iaitu:

3.4.1 Penerima emel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;

3.4.2 Penerima mesti membuat akuan penerimaan emel rahsia rasmi sebaik sahaja menerimanya;

3.4.3 Emel rahsia rasmi bertanda *Rahsia Besar* dan *Rahsia* tidak boleh dimajukan kepada pihak lain. Sementara emel bertanda *Sulit* dan *Terhad* yang hendak dimajukan kepada pihak lain memerlukan izin daripada pemula dokumen;

3.4.4 Emel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan hendaklah berpandukan Dasar Pengurusan Rekod dan arkib Negara dengan merujuk perkara 3.8 iaitu Pemusnahan Rekod Elektronik; dan

3.4.5 Jabatan perlu menentukan sistem emel rahsia rasmi yang disambungkan kepada Internet atau intranet mesti mempunyai sistem keselamatan yang mencukupi seperti *Firewall.*

4.0 KESELAMATAN DARI ANCAMAN VIRUS

Serangan virus komputer merupakan masalah besar yang hadapi oleh JKSM/JKSN/MSN dan di lain-lain organisasi. Semua pengguna dikehendaki mengambil langkah-langkah berikut:

4.1.1 Pengguna mestilah sentiasa melakukan imbasan nyah virus *(virus scanning)* terhadap semua media yang dibawa dari luar seperti *thumb drive, external hard disk* untuk pengesahan sama ada terdapat virus atau tidak;

4.1.2 Pengguna dimestikan untuk menggunakan perisian anti-virus yang sah;

4.1.3 Pengguna adalah dikehendaki melakukan imbasan nyah virus sekerap yang mungkin atau secara berkala terhadap komputer dan *notebook* yang digunakan bagi memastikan ia bebas dari virus;

4.1.4 Sekiranya terdapat serangan atau jangkitan virus ke atas dokumen atau komputer, sila laporkan kepada pasukan Pentadbir Sistem di fasiliti masing-masing; dan

4.1.5 Pengguna komputer *tablet* dan *notebook* hendaklah sentiasa memastikan kemudahan tanpa wayar (seperti *bluetooth, wifi)* dinyahaktifkan sekiranya tidak digunakan bagi mengurangkan insiden ancaman keselamatan.

5.0 PENGGUNAAN DAN PENGURUSAN RANGKAIAN

5.1 Infrastruktur Rangkaian

5.1.1 Penggunaan rangkaian di JKSM/JKSN/MSN hanya dibenarkan untuk warga JKSM/JKSN/MSN sahaja. Pengguna luar yang hendak menggunakan kemudahan rangkaian JKSM/JKSN/MSN hendaklah mendapatkan kebenaran Pentadbir Rangkaian JKSM/JKSN/MSN;

5.1.2 Fasiliti yang telah dirangkaikan melalui 1Gov*Net tidak dibenarkan menggunakan rangkaian yang lain (seperti jalur lebar) kecuali mendapat kelulusan Bahagian Teknologi Maklumat dan Komunikasi (BTMK) dengan mematuhi syarat-syarat yang telah ditetapkan;

5.1.3 Fasiliti JKSM disarankan mengguna *firewall*, *Intrusion Prevention System (IPS)* dan *content filtering* bagi memastikan rangkaian JKSM dilindungi dari sebarang ancaman keselamatan;

5.1.4 Rangkaian setempat (LAN) di fasiliti hanya boleh diintegrasikan antara talian 1Gov*Net dan egNet sahaja. Manakala talian lain tidak dibenarkan kecuali dengan mendapat kebenaran dari BTMK;

5.1.5 Setiap peralatan ICT yang dirangkaikan ke talian 1Gov*Net tidak boleh disambungkan ke rangkaian lain pada masa yang sama seperti jalur lebar *(broadband)* dan sebagainya;

5.1.6 Penggunaan rangkaian tanpa wayar setempat *(wireless LAN)* di fasiliti disarankan dilengkapi dengan ciri-ciri keselamatan seperti menggunakan sekurang-kurangnya pengesahan *WPA2* pada peralatan *wireless* dan *radius server*;

5.1.7 Sebarang permohonan berkaitan dengan perkhidmatan rangkaian seperti *ftp, netting, DNS, port* dan lain-lain perlu dikemukakan secara rasmi dengan mengisi Borang Permohonan Pembukaan Port (*Firewall Services Configuration Request Form*–JKSM/BTMK/BRG/2013/01) dan kemukakan kepada Pentadbir Rangkaian BTMK selewat-lewatnya tiga (3) hari sebelum perkhidmatan diperlukan;

5.1.8 Sekiranya *DNS, netting* dan *port* yang diperlukan tidak digunakan lagi, pihak Pentadbir Rangkaian BTMK perlulah dimaklumkan bagi tujuan memperkemaskini.

5.2 Tanggungjawab Pentadbir Rangkaian

5.2.1 Memastikan rangkaian 1Gov*Net sentiasa boleh digunakan;

5.2.2 Menyelesaikan masalah rangkaian 1Gov*Net;

5.2.3 Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal;

5.2.4 Mengenalpasti dan mengemaskini *firewall rules* yang telah ditetapkan sahaja;

5.2.5 Pemantauan aktiviti capaian pengguna 1Gov*Net dari masa ke semasa;

5.2.6 Mengemaskini dan menambahbaik reka bentuk infrastruktur 1Gov*Net mengikut polisi keselamatan yang telah ditetapkan;

5.2.7 Mengenalpasti aktiviti-aktiviti yang tidak normal seperti penggunaan rangkaian yang tinggi dengan membuat capaian ke laman yang tidak dibenarkan;

5.2.8 Memantau laluan trafik rangkaian dari masa ke semasa dan mengambil tindakan yang sewajarnya dengan kadar segera jika berlaku kesesakan trafik rangkaian atau rangkaian tidak dapat berfungsi dengan baik;

5.2.9 Mengawal IP pengguna serta mengambil tindakan terhadap pengguna sekiranya berlaku penyalahgunaan IP;

5.2.10 Mengawal dan sentiasa mengemaskini DNS dari masa ke semasa;

5.2.11 Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

5.3 Pengurusan Alamat Internet Protokol (IP)

5.3.1 Sebarang permohonan untuk menggunakan IP Statik hendaklah diperolehi daripada Pentadbir Rangkaian di fasiliti masing-masing;

5.3.2 Pengguna adalah dilarang sama sekali untuk menukar IP di dalam peralatan ICT masing-masing tanpa kebenaran Pentadbir Rangkaian di fasiliti masing-masing;

5.3.3 Sebarang pertukaran pengguna yang menggunakan IP statik hendaklah dimaklumkan kepada Pentadbir Rangkaian di fasiliti masing-masing;

5.3.4 IP statik yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan IP statik yang diberi, Pentadbir Rangkaian yang bertanggungjawab di fasiliti masing-masing berhak mengeluarkan pengguna tersebut dari rangkaian.

5.4 Sambungan Rangkaian

5.4.1 Semua permohonan baru untuk mendapatkan sambungan rangkaian LAN mestilah melalui Pentadbir Rangkaian di fasiliti masing-masing;

5.4.2 Pengguna tidak dibenarkan memutuskan/menyambung sambungan kabel fizikal UTP pada mana-mana *port* dalam rak peralatan rangkaian tanpa kebenaran dari pihak Pentadbir Rangkaian di fasiliti masing-masing;

5.4.3 Pengguna tidak dibenarkan menukar maklumat yang terdapat pada UTP *port*;

5.4.4 Perbuatan yang boleh merosakkan UTP *port*, kabel UTP atau rak rangkaian serta peralatannya adalah dilarang;

5.4.5 Sebarang kerosakan pada kabel UTP, *network point* dan *network port* pada mana-mana *switch/hub* hendaklah dilaporkan kepada Pentadbir Rangkaian di fasiliti masing-masing.

5.5 Jalur Lebar *(Broadband)* / Rangkaian Tanpa Wayar (*wireless*)

5.5.1 Kemudahan *broadband* hanya diberikan untuk tujuan rasmi;

5.5.2 Permohonan perkhidmatan *mobile broadband* bagi tujuan rasmi di luar pejabat hendaklah mengemukakan permohonan kepada Bahagian Teknologi Maklumat dan Komunikasi;

5.5.3 Pengguna di fasiliti JKSM yang menggunakan 1Gov*Net tidak dibenarkan menggunakan *broadband;*

5.5.4 Pengguna yang telah menggunakan kemudahan selain 1Gov*Net seperti *broadband/wireless,* dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula ke rangkaian JKSM.

5.6 *File Transfer Protocol* (FTP)

Penggunaan FTP hendaklah dilaksanakan dengan ciri-ciri keselamatan yang disarankan seperti menggunakan aplikasi *putty* bagi sistem pengoperasian *Linux*, *sftp* bagi sistem pengoperasian *Windows , SSL, VPN* dan sebagainya yang bersesuaian.

6.0 KESELAMATAN KATA LALUAN

Bagi menjamin keselamatan kata laluan pengguna perlulah mematuhi prosedur berikut:

6.1.1 Rahsiakan kata laluan. Kata laluan hendaklah dihafal dan jangan sekali-kali disalin atau di papar di mana-mana media seperti buku catatan, *thumbdrive*, CD dan sebagainya kerana dikhuatiri akan diketahui dan disalahgunakan oleh orang lain;

6.1.2 Gunakan kata laluan yang kukuh melalui gabungan nombor, huruf, tanda dan simbol yang mempunyai sekurang-kurangnya dua belas (12) aksara (contoh: P6swO~d!1234). (AMARAN: Jangan guna kata laluan ini kerana ianya telah diketahui umum);

6.1.3 Kata laluan perlu ditukar dalam tempoh 90 hari;

6.1.4 Elakkan dari menggunakan semula empat (4) kata laluan yang terdahulu;

6.1.5 ID pengguna tidak boleh digunakan sebagai kata laluan;

6.1.6 Elakkan menggunakan kata laluan yang mengandungi maklumat yang berkaitan dengan pengguna, peralatan dan perisian yang diguna pakai;

6.1.7 Menukar serta merta kata laluan asal *(default password)* yang diterima daripada Pentadbir Sistem; dan

6.1.8 Sekiranya kata laluan telah dicerobohi atau disyaki dicerobohi, kakitangan JKSM hendaklah melaporkan kepada JKSMCERT dengan serta merta.

7.0 KESELAMATAN RANGKAIAN (*Network Security*)

7.1.1 Pentadbir Rangkaian di setiap fasiliti JKSM perlu menyedia dan mengemaskini reka bentuk rangkaian untuk tujuan merancang, memantau dan menyenggara rangkaian;

7.1.2 Pengguna perlu mematuhi perkara 1.2 dan perkara 4.0. Tindakan disiplin akan diambil sekiranya ada penyalahgunaan kemudahan ICT seperti memuat turun perisian tanpa kebenaran kerana ini akan menjejaskan prestasi rangkaian *(network performance)* dan pendedahan rangkaian kepada ancaman keselamatan seperti virus;

7.1.3 *Firewall rules* hendaklah disediakan dan sentiasa dikemaskini di semua fasiliti JKSM bagi tujuan mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan aset-aset ICT di dalam rangkaian JKSM daripada ancaman keselamatan oleh pihak yang tidak bertanggungjawab;

7.1.4 Pentadbir Sistem bertanggungjawab memantau laporan log di setiap server untuk memastikan tiada capaian yang tidak sah dibuat ke atas server berkenaan;

7.1.5 Pengguna hendaklah menggunakan teknologi VPN bagi memastikan keselamatan maksimum semua maklumat yang dihantar dan diterima melalui transaksi atas talian jika ingin membuat capaian rangkaian antara fasiliti JKSN/MSN dengan Ibu Pejabat JKSM yang berpusat di Putrajaya;

7.1.6 *Proxy* atau *webcache server* dan *viruswall server* perlu diwujudkan bagi mengawal serta memantau penggunaan Internet dari rangkaian JKSM. Ia berfungsi mengawal pengguna membuat

capaian laman web serta muat turun fail yang tidak dibenarkan seperti gambar lucah, *screen saver*, lagu, video dan sebagainya.

8.0 KESELAMATAN FIZIKAL PERKAKASAN ICT JKSM

Sebagai satu langkah bagi memastikan keselamatan perkakasan ICT JKSM berada di dalam tahap maksima, pengguna hendaklah sentiasa mematuhi garis panduan berikut:

8.1.1 Setiap komputer, komputer *tablet* atau *notebook* mestilah mempunyai kata laluan yang kukuh;

8.1.2 Setiap komputer, *notebook* dan *server* mestilah dilakukan pengemaskinian *patches* dan *services pack Microsoft Windows / Open Source* yang terkini;

8.1.3 Setiap server, komputer dan *notebook* hendaklah menggunakan perisian yang sah seperti antivirus, sistem pengoperasian dan lain- lain;

8.1.4 Setiap *server*, komputer dan *notebook* hendaklah mempunyai nama komputer dan dilarang mengubah atau meminda nama komputer dan konfigurasi dalam komputer yang disediakan tanpa kebenaran;

8.1.5 Setiap perolehan perkakasan ICT hendaklah yang tulen serta dari pengedar yang sah dan berdaftar (bukan klon);

8.1.6 Pastikan perkakasan ICT pejabat tidak digunakan oleh orang yang tidak berkenaan dan hanya untuk urusan rasmi sahaja;

8.1.7 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 A*utomatic Voltage Regulator (AVR)* untuk memastikan bekalan elektrik sentiasa dibekalkan mengikut spesifikasi keperluan komputer/*notebook*;

8.1.8 Pastikan komputer atau *notebook* tidak terdedah secara terus kepada pancaran matahari/haba dan elakkan komputer daripada kawasan tarikan kuasa magnet serta kuasa voltan yang tinggi;

8.1.9 Pastikan bekalan punca elektrik ditutup semasa penyambungan peralatan komputer dan aksesorinya atau setelah selesai penggunaannya;

8.1.10 Pastikan komputer atau *notebook* diletakkan di tempat dingin dan kering persekitarannya serta di tempat yang selamat;

8.1.11 Konfigurasikan komputer atau *notebook* kepada *sleeping mode* jika digunakan secara berterusan;

8.1.12 Tamatkan aplikasi tanpa tindakbalas *(not responding)* dengan kekunci **Ctrl-Alt-Del** jika komputer gagal berfungsi dengan baik seperti *hang*;

8.1.13 Pastikan komputer atau *notebook* mempunyai sistem masa dan tarikh yang betul untuk tujuan audit dan penghantaran emel;

8.1.14 Sentiasa keluar daripada tetingkap *(windows)* atau mematikan komputer dengan cara yang betul bagi mencegah ralat sistem. Tidak dibenarkan mematikan komputer secara fizikal iaitu dengan menutup suis atau mencabut *plug* dengan begitu sahaja;

8.1.15 Dilarang menghentak/mengetuk dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer, *notebook* atau sebarang perkakasan ICT;

8.1.16 Sentiasa mempunyai salinan pendua *(backup)* bagi data-data penting yang terdapat di dalam komputer;

8.1.17 Pengguna adalah dilarang membaiki sebarang kerosakan terhadap perkakasan ICT tanpa kebenaran bagi mengelakkan kehilangan terus maklumat yang tersimpan di dalamnya pengguna tidak dibenarkan menggunakan ID *Administrator* kecuali mendapat kebenaran dan tidak dibenarkan membuang instalasi (*uninstall)* mana-mana perisian yang telah dipasang; dan

8.1.18 Pengguna yang tidak menggunakan komputer atau *notebook* buat sementara waktu, maka *lock computer* hendaklah dilakukan.

9.0 TATACARA PENGURUSAN MEDIA STORAN

9.1.1 Pengguna hendaklah memastikan media storan yang dibekalkan hanya untuk kegunaan urusan rasmi JKSM;

9.1.2 Setiap media perlulah dilabelkan mengikut Bahagian/Unit/Nama;

9.1.3 Media yang mengandungi maklumat atau rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad atau Rahsia;

9.1.4 Pengguna adalah dilarang menyalin, membawa keluar atau memberi media yang mengandungi maklumat rahsia rasmi kepada orang lain. Ini adalah untuk mengelak dari berlakunya pembocoran rahsia;

9.1.5 Pengguna disarankan untuk melakukan kaedah pemampatan *(compress)* untuk mengurangkan saiz fail bagi memaksimakan penggunaan media storan;

9.1.6 Media yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadamkan *(delete)* sebelum digunakan untuk tujuan yang lain;

9.1.7 Pengguna hendaklah memastikan keselamatan fizikal terhadap media dari ancaman seperti sinaran matahari, suhu panas, elektrostatik dan magnet serta disimpan di tempat yang selamat. Ini dapat mengelakkan maklumat atau data menjadi rosak *(corrupted)* atau tidak boleh dibaca;semua media storan yang rosak atau tidak boleh digunakan lagi, perlulah di format semula

untuk memadamkan kesemua data di dalamnya sebelum dilupuskan dan dimusnahkan;

9.1.8 Setiap media storan mestilah sentiasa diimbas sebelum digunakan;

9.1.9 Pengguna tidak digalakkan untuk berkongsi penggunaan media storan bagi mengelakkan maklumat yang disimpan di dalam media storan diakses oleh pengguna yang tidak berhak; dan

9.1.10 Sebarang kehilangan dan ancaman terhadap maklumat yang terkandung di dalam media atau kehilangan media hendaklah dilaporkan kepada JKSMCERT.

10.0 KESELAMATAN PERKAKASAN ICT DI PUSAT DATA/ BILIK SERVER JKSM

Berikut ialah beberapa langkah yang perlu dilaksanakan bagi melindungi *server* tersebut seperti:

10.1.1 Setiap Pusat Data/Bilik Server hendaklah disediakan dengan sistem *Security Access Door* atau sentiasa berkunci bagi memantau dan mengawal pengguna yang keluar masuk ke bilik *server*;

10.1.2 Hanya pengguna yang dibenarkan sahaja boleh memasuki bilik *server*;

10.1.3 Setiap *server* mestilah dilabelkan bagi memudahkan setiap pentadbir menjalankan tugas masing-masing;

10.1.4 Pastikan bilik *server* sentiasa bersih, kemas, tidak menempatkan perkakasan yang tidak diperlukan dan *server* tidak terdedah kepada habuk;

10.1.5 Pastikan pengkabelan disusun dengan kemas dan teratur serta dilabelkan dengan betul;

10.1.6 Penghawa dingin mestilah berfungsi dengan baik di mana suhunya di dalam lingkungan ±19.5°C dan kelembapan di paras 50.7%;

10.1.7 Semua peralatan keselamatan, UPS, penghawa dingin mestilah diselenggarakan secara berkala;

10.1.8 Diagram kedudukan *server* hendaklah disediakan dan dipamerkan di dalam Pusat Data/Bilik Server JKSM; dan

10.1.9 Semua pergerakan keluar dan masuk perkakasan di Pusat Data perlu direkodkan dan mendapat kebenaran dengan menggunakan borang permohonan yang disediakan

11.0 KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA

Beberapa langkah telah dikenal pasti dan dilaksanakan bagi melindungi aset-aset tersebut. Antaranya adalah:

11.1 Pembaik Pulih Sistem

Pembaik pulih sistem adalah merupakan proses baik pulih akibat dari kemusnahan atau kehilangan data yang berlaku disebabkan beberapa faktor. Antaranya adalah seperti yang berikut:

11.1.1 kegagalan server berfungsi;
11.1.2 kerosakan fizikal *hard disk*; dan
11.1.3 masalah kesilapan dalam *programming*

Proses pembaik pulih sistem terbahagi kepada dua peringkat iaitu prosedur salinan pendua *(backup)* dan prosedur baik pulih *(restore).*

11.2 Prosedur Salinan Pendua *(Backup)*

11.2.1 *Backup* keseluruhan semua data dan aplikasi termasuk *Operating System* (OS) hendaklah dibuat sekurang-kurangnya pada setiap minggu untuk semua server berpandukan prosedur-prosedur *backup* yang telah ditetapkan. Namun *backup* keseluruhan secara bulanan wajib dilakukan.

Walau bagaimanapun, kekerapan penjanaan data *backup* adalah mengikut kepentingan data-data tersebut secara berperingkat dari harian hinggalah bulanan.

11.2.2 *Backup* atau salinan data ke dalam media storan perlu dilakukan setiap hari bagi sebarang perubahan atau *incremental data* untuk mengelakkan kehilangan data sekiranya berlaku kerosakan *hard disk;*

11.2.3 Semua *backup* yang dilakukan hendaklah direkod, dilabel secara unik dan disimpan di tempat yang selamat. Ini adalah untuk memudahkan carian fail dari semasa ke semasa;

11.2.4 *Backup* sistem aplikasi dan sistem operasi perlu diadakan sekurang-kurangnya sekali bagi setiap keluaran versi terbaru dari semasa ke semasa mengikut peraturan yang ditetapkan semasa perisian itu dibangunkan atau diperoleh atau mengikut garis panduan yang dikeluarkan dari semasa ke semasa. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam menentukan kekerapan *backup;*

11.2.5 *Backup* untuk data dan sistem aplikasi/sistem operasi dicadangkan dibuat dalam dua (2) salinan dan setiap satu disimpan di lokasi yang berlainan. Lokasi-lokasi tersebut adalah :-

11.2.5.1 Lokasi *on-site* - di mana sistem tersebut beroperasi.

11.2.5.2 Lokasi *off-site* di bangunan lain yang berdekatan atau mana-mana Jabatan Kerajaan lain yang berdekatan dan mempunyai kemudahan keselamatan untuk menyimpan media *backup*.

11.2.5.3 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.

11.2.5.4 Setiap media b*ackup* yang dilakukan hendaklah diuji *(on-site dan off-site)* sekurang-kurangnya sekali setahun. Ini adalah bagi memastikan media backup tersebut berfungsi dengan baik *(readable and usable)* untuk tujuan baik pulih.

11.2.5.5 *Standard Operating Procedure* (SOP) bagi setiap perkhidmatan ICT seperti aplikasi, rangkaian dan lain- lain hendaklah disediakan bagi memastikan kesinambungan perkhidmatan. Pengujian SOP hendaklah dilaksanakan sekurang-kurangnya setahun sekali.

11.3 Prosedur Baik Pulih *(Restore)*

Dengan prosedur *backup* di atas, proses pembaik pulih boleh dilakukan sama ada dari peringkat paling kritikal seperti kegagalan seluruh *partition hard disk* atau pangkalan data, aplikasi, direktori sehingga ke atas fail tertentu dapat dibaik pulih dengan mudah dan selamat.

11.4 Pelan Pemulihan Bencana (Disaster Recovery Plan)

Data-data kritikal disalin *(backup* di para 11.2*)* ke dalam media storan dan disimpan di bilik *server*. Di samping itu salinan pendua bagi data-data tersebut perlu dihantar dan disimpan di lokasi *off- site* sebagai salah satu pelan pemulihan bencana. Kaedah 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 sebagainya.

12.0 PEMBANGUNAN SISTEM APLIKASI

12.1.1 Memastikan *vendor* yang dilantik mengetahui dan menggunakan tentang *"Secured Coding"* jika perlu;

12.1.2 Mengubah konfigurasi asal *(default)* termasuk kata laluan, *port* dan sebagainya;

12.1.3 Memastikan *vendor* menyediakan dan menyerahkan *Standard of Procedure* (SOP*)* bagi setiap aplikasi yang dibangunkan;

12.1.4 Menutup *directory listing* setiap aplikasi kepada umum bagi mengelak data mudah dijejaki oleh pihak yang tidak bertanggungjawab;

12.1.5 Memastikan *vendor* menyerahkan semua kata laluan berkaitan aplikasi seperti kata laluan pangkalan data dan *server*;

12.1.6 Tidak menggunakan *IP address* sebagai URL bagi membuat capaian dan menutup *IP address* daripada diketahui oleh umum;

12.1.7 Menutup akses *anonymous*;

12.1.8 Memastikan *port* yang diperlukan adalah untuk kegunaan aplikasi tersebut sahaja berfungsi. Penggunaan *port* seperti *port* 445 hendaklah dielakkan daripada digunakan kerana ianya merupakan *file sharing* dan mudah menyebarkan virus;

12.1.9 Setiap aplikasi perlu direka dengan fungsi menguatkuasakan tamat masa sesi yang terbiar (*idle timeout*), iaitu apabila tiada

aktiviti pengguna untuk tempoh masa yang tertentu, sesi akan ditamatkan;

12.1.10 Pengguna perlu log masuk semula selepas penamatan *idle timeout* tersebut. Saranan bagi tempoh tamat masa adalah 15 minit;

12.1.11 Pengujian secara terperinci hendaklah dilakukan ke atas aplikasi atas talian terutamanya semasa input data bagi mengatasi masalah *web defacement* dan sebagainya;

12.1.12 Setiap sistem aplikasi mestilah disediakan dengan *log file* dan *audit trail*;

12.1.13 Setiap aplikasi sistem yang dibangunkan sentiasa mengemaskini *security patches* dan menggunakan versi terkini seperti penggunaan *Content Management System (CMS)* iaitu *Joomla*;

12.1.14 Memastikan sistem pangkalan data dan perisian pembangunan aplikasi hendaklah menggunakan *features* terkini;

12.1.15 Memastikan dokumentasi sistem aplikasi disediakan dan dikemaskini dari semasa ke semasa;

12.1.16 Sebarang perubahan kepada ahli pasukan sistem aplikasi hendaklah dimaklumkan.

13.0 PRASARANA KUNCI AWAM KERAJAAN (GPKI)

Semua sistem ICT kerajaan yang memerlukan kemudahan Prasarana Kunci Awam (PKI) hendaklah menggunakan perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI). Pelaksanaan Prasarana Kunci Awam Kerajaan (GPKI) ini hendaklah berpandukan kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)].

14.0 PERANAN DAN TANGGUNGJAWAB SEMUA FASILITI JKSM

Semua fasiliti JKSM memainkan peranan yang penting bagi memastikan penggunaan dan keselamatan ICT JKSM berada dalam tahap yang paling maksimum sepanjang masa.

15.0 KHIDMAT NASIHAT

Sebarang pertanyaan dan kemusykilan berkaitan dengan garis panduan ini bolehlah dirujuk kepada Bahagian Teknologi Maklumat dan Komunikasi. Permohonan untuk keterangan lanjut mengenai kandungan dokumen ini bolehlah diajukan kepada:

Bahagian Teknologi Maklumat dan Komunikasi,
Jabatan Kehakiman Syariah Malaysia (JKSM),
Aras 4, Blok C,
No 20, Lot PT 12075,
Jalan Tunku Abdul Rahman,
Kompleks Islam Putrajaya,
62100, Presint 3,
Putrajaya.

16.0 PENUTUP

Garis panduan ini merupakan amalan-amalan terbaik dalam pengendalian keselamatan ICT dan mesti dipatuhi oleh semua pengguna di JKSM/JKSN/MSN. Garis panduan ini akan dikemaskini dari semasa ke semasa selaras dengan arus perkembangan teknologi maklumat dan komunikasi serta perundangan.