



# **JABATAN PENDAFTARAN NEGARA MALAYSIA**

**No. 20, Persiaran Perdana, Presint 2,  
62551 W.P Putrajaya.**

## **PROCEDURE MANUAL**

**Document Title: GARIS PANDUAN MENGENAI  
TATACARA PENGGUNAAN INTERNET DAN MEL  
ELEKTRONIK**

**Document Number: PS-JPN-SM-PS-22 (BM)**

**MS ISO 27001:2005**

<b>Reviewed &amp; Verified By:</b>	<b>Approved By:</b>
<p>.....</p> <p><b>Name :</b></p> <p><b>Designation :</b></p> <p><b>Date :</b></p>	<p>.....</p> <p><b>Name :</b></p> <p><b>Designation :</b></p> <p><b>Date :</b></p>



## **KANDUNGAN**

<b>1.0</b>	<b>PENGENALAN.....</b>	<b>ERROR! BOOKMARK NOT DEFINED.</b>
<b>2.0</b>	<b>TUJUAN.....</b>	<b>E</b>
	rror! Bookmark not defined.	
<b>3.0</b>	<b>TATACARA PENGGUNAAN INTERNET .....</b>	<b>3</b>
<b>4.0</b>	<b>TATACARA PENGGUNAAN MEL ELEKTRONIK.....</b>	<b>6</b>
<b>5.0</b>	<b>KAWALAN KESELAMATAN INTERNET DAN E-MEL.....</b>	<b>9</b>
<b>6.0</b>	<b>TANGGUNGJAWAB PENTADBIR E-MEL DAN INTERNET .....</b>	<b>10</b>
<b>7.0</b>	<b>TANGGUNGJAWAB PENGGUNA .....</b>	<b>12</b>
<b>8.0</b>	<b>KELAYAKAN DAN PENGHADAN .....</b>	<b>13</b>
<b>9.0</b>	<b>KHIDMAT NASIHAT .....</b>	<b>13</b>
<b>10.0</b>	<b>PENUTUP.....</b>	<b>14</b>
	<b>APPENDIX A-DOCUMENT AMENDMENT REGISTER.....</b>	<b>15</b>



## 1.0 PENGENALAN

Perkembangan teknologi maklumat dan komunikasi (ICT) telah membolehkan maklumat dihantar dan diterima dengan pantas. Kemudahan ini telah membawa kepada peningkatan penggunaan internet dan mel elektronik atau e-mel dalam sektor awam. Hakikat ini turut dipengaruhi oleh bilangan pengguna dan kepentingan maklumat yang kian meningkat dari semasa ke semasa.

Komunikasi secara elektronik juga dilihat sebagai salah satu saluran penting dalam membantu mewujudkan perkongsian maklumat. Tambahan pula, kaedah ini membolehkan proses penghantaran dan penerimaan sesuatu maklumat dilaksanakan dengan lebih cepat dan mudah. Bagaimanapun, pengurusan internet dan e-mel yang tidak terkawal boleh menjejaskan keselamatan maklumat. Justeru, perlindungan keselamatan yang bijaksana perlu diwujudkan dan disesuaikan bagi menjamin kesahihan, keutuhan dan kebolehsediaan maklumat yang berterusan.

## 2.0 TUJUAN

Tujuan utama garis panduan ini ialah untuk menerangkan tatacara penggunaan internet dan e-mel, meningkatkan tahap keselamatan sistem komunikasi dokumen rasmi Kerajaan dan mengurangkan risiko gangguan operasi internet dan e-mel.

## 3.0 TATACARA PENGGUNAAN INTERNET

3.1 Teknologi internet telah memudahkan perhubungan antara pengguna dan menyediakan akses kepada banyak maklumat dalam pelbagai bentuk format dengan menyediakan sumber pembelajaran, rekreasi, penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Perkhidmatan Awam dalam usahanya menuju ke arah pemodenan tadbiran telah melihat internet sebagai satu *platform* untuk penambahbaikan perkhidmatan yang disediakan. Dalam konteks ini, kakitangan Jabatan Pendaftaran Negara (JPN) perlu menggunakan kemudahan internet dengan cara yang bertanggungjawab dan konsisten.

3.2 Internet adalah infrastruktur saluran global dan merupakan punca maklumat yang tidak terkawal. Dengan sebab itu, ketepatan maklumat internet tidak boleh ditentukan. Justeru, kakitangan JPN perlu memainkan peranan dan bertindak secara bijak menilai kesahihan, ketepatan dan kesesuaian sesuatu maklumat yang diperolehi



agar kerja yang dilaksanakan tidak menyimpang dari tujuan sebenar jabatan.

3.3 Penggunaan internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai pelanggaran tatacara yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan sistem ICT dan pengurusan rekod elektronik, mengganggu sistem rangkaian ICT dan merosakkan imej Perkhidmatan Awam. Oleh yang demikian, bagi menjamin kemudahan internet digunakan dengan selamat, adalah wajar JPN menentukan latihan yang bersesuaian, penggunaan teknologi yang kukuh dan dasar yang menyeluruh agar pelanggaran seumpamanya tidak berlaku.

3.4 Berikut adalah tatacara yang mesti diikuti dalam menggunakan internet.

**(a) Hak Akses Pengguna**

Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan oleh JPN untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan. Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk maklumat) adalah hak milik Kerajaan.

**(b) Privasi Pengguna**

Setiap pengguna hendaklah menghormati privasi pengguna lain dengan tidak menimbulkan sebarang gangguan seperti mencapai fail, memecah kata laluan, memasuki sistem komputer dan mengubah komponen perisian tanpa kebenaran.

**(c) Mengenal pasti Identiti Pengguna**

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

**(d) Memilih Laman**

Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan sahaja.

**(e) Pengesahan Maklumat**

Bahan yang diperolehi dari internet perlulah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber internet hendaklah juga dinyatakan.

**(f) Muat Naik Bahan (Upload)**

Bahan rasmi yang hendak dimuat naik ke internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik.

**(g) Muat Turun Bahan (Download)**

Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan sahaja.

**(h) Perbincangan Awam**

Hanya kakitangan JPN yang mendapat kebenaran sahaja boleh melibatkan diri dan menggunakan kemudahan ini. Kandungan perbincangan awam seperti *newsgroup* dan *bulletin board* mestilah mendapat pengesahan daripada Ketua Jabatan. Perlu diingat bahawa setiap maklumat yang dikongsi melambangkan imej Jabatan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan.

3.5 Kakitangan JPN adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan internet seperti:

- (a) Merosak dan mengancam keselamatan dengan menggunakan hak akses pengguna lain untuk mencapai sistem komputer, mendapatkan maklumat dan mengubah komponen sistem tanpa kebenaran;
- (b) memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen;
- (c) menyedia dan menghantar maklumat berulang-ulang berupa gangguan;
- (d) menyedia, memuat naik, memuat turun, menyimpan dan menyebarkan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah, ganas dan berbau perkauman;
- (e) menyedia, memuat naik, memuat turun, menyimpan dan menyebarkan maklumat internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan;
- (f) menyalahgunakan kemudahan perbincangan awam atas talian seperti



*newsgroup dan bulletin board;*

- (g) memuat naik, memuat turun, menyimpan dan menyebarkan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna internet yang lain;
- (h) memuat turun, menyimpan, menyebarkan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;
- (i) menggunakan kemudahan *chatting* melalui internet;
- (j) menjalankan aktiviti-aktiviti komersial dan politik;
- (k) melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas;
- (l) memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepingan fail melebihi saiz 2 megabait yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer;
- (m) menggunakan kemudahan modem atau broadband untuk membuat capaian terus ke internet tanpa kelulusan Ketua Jabatan; dan
- (n) mengubah konfigurasi komputer seperti menukar IP atau segmen-segmen rangkaian (VLAN) tanpa kelulusan Ketua Jabatan yang bertujuan untuk mendapatkan capaian internet.

#### 4.0 TATACARA PENGGUNAAN MEL ELEKTRONIK

4.1 Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. Aplikasi e-mel ini digunakan secara meluas dan membenarkan komunikasi lebih daripada dua hala dengan cara yang pantas dan lebih sesuai untuk penulisan yang ringkas.

4.2 E-mel rasmi yang digunakan adalah untuk tujuan rasmi dan didaftarkan di bawah domain JPN. Salah satu contoh alamat e-mel rasmi ialah [ahmad@jpn.gov.my](mailto:ahmad@jpn.gov.my). E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

##### (a) E-mel Rahsia Rasmi

E-mel yang 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*.

**(b) E-mel Bukan Rahsia Rasmi**

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

4.3 Adalah digalakkan alamat e-mel khusus diwujudkan bagi memudahkan orang ramai berhubung dengan JPN sekiranya memerlukan penjelasan lanjut, membuat aduan atau mengemukakan pandangan. Contoh alamat e-mel khusus JPN ialah [admin@jpn.gov.my](mailto:admin@jpn.gov.my).

4.4 Berikut adalah kaedah penggunaan e-mel yang betul.

**(a) Pemilikan Akaun E-mel**

Pemilikan akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan. Akaun atau alamat e-mel yang diperuntukkan oleh jabatan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.

**(b) Format**

Penggunaan huruf besar kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika. Sebaik-baiknya, gabungan huruf besar dan huruf kecil digunakan dan dipraktikkan di tempat-tempat yang bersesuaian di samping mengamalkan penggunaan bahasa yang betul, ringkas dan sopan.

Pengguna juga perlu memastikan bahawa subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan.

**(c) Penghantaran**

Penghantaran e-mel rasmi hendaklah menggunakan akaun e - mel rasmi dan pastikan alamat e-mel penerima adalah betul. Penghantar boleh menggunakan kemudahan 'salinan kepada' (cc) sekiranya e-mel tersebut perlu dimaklumkan kepada penerima lain. Bagaimanapun, penggunaan 'blind cc' (bcc) tidak digalakkan.

Kemudahan 'reply' digunakan untuk menjawab e-mel kepada penghantar asal dan 'forward' untuk memanjangkan e-mel atau dimajukan kepada penerima lain. Sebagai amalan baik, e-mel penghantar hendaklah dijawab **selewat-lewatnya 4 hari** dari tarikh e-mel berkenaan diterima.

**(d) Penghantaran Bersama Fail Kepilan**

Penghantar hendaklah mengamalkan penggunaan fail kepil, misalnya mengepilkan fail minit mesyuarat dan elakkan dari menghantar dan menerima fail e-mel yang bersaiz melebihi 2 megabait. Sekiranya perlu, kaedah pemampatan untuk mengurangkan saiz fail adalah disarankan.

**(e) Penerimaan**

Pengguna seharusnya mengelakkan dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui.

**(f) Mengenal Pasti Identiti Pengguna**

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

**(g) Penyimpanan**

Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik.

Pengguna hendaklah memastikan jumlah e-mel yang disimpan di dalam kotak masuk e-mel adalah tidak melebihi ruang storan yang telah diperuntukkan dan mengutamakan penyimpanan e-mel yang perlu sahaja. Penyimpanan salinan e-mel pada sumber storan kedua adalah digalakkan bagi tujuan keselamatan dan harus diletakkan di tempat yang selamat.

**(h) Pemusnahan dan Penghapusan**

E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan. (Contoh: draf kertas kerja, draf minit, kertas makluman dan brosur).

**(i) Tarikh dan Masa Sistem Komputer**

Sebelum sesuatu mesej dihantar, perlu ditentukan tarikh dan masa sistem komputer adalah tepat.

4.5 Berikut Pengguna adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel rasmi Jabatan seperti:

- (a) menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

Title: GARIS PANDUAN MENGENAI  
TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK

- (b) menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;
- (c) menggunakan e-mel untuk tujuan komersial atau politik;
- (d) menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;
- (e) menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, e-mel sampah, e-mel bom, e-mel *spam*, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Malaysia;
- (f) menyebarkan kod perosak seperti virus, *worm*, *trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;
- (g) menghantar semula e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian; dan
- (h) membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.

## 5.0 KAWALAN KESELAMATAN INTERNET DAN E-MEL

Internet dan e-mel adalah terdedah kepada ancaman seperti pencerobohan, penyelewengan, pemalsuan, pemintasan dan pembocoran rahsia. Dengan itu, keselamatan internet dan e-mel perlu untuk melindungi maklumat rahsia rasmi dan maklumat bukan rahsia rasmi Kerajaan dari capaian tanpa kuasa yang sah. Keselamatan internet dan e - mel bergantung kepada faktor-faktor sokongan berikut.

### (a) Keselamatan Fizikal

Komputer hendaklah diletakkan di tempat yang mempunyai kawalan fizikal yang selamat daripada penceroboh atau sebarang bentuk capaian tidak sah.

### (b) Keselamatan Dokumen Elektronik

Bagi memastikan semua fail yang dihantar dan diterima bebas daripada sebarang bentuk ancaman keselamatan, perisian anti-virus dan penapis *malicious codes* perlulah dikemas kini dari semasa ke semasa.

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".

Sekiranya penyelenggaraan komputer hendak dilaksanakan, kakitangan yang bertanggungjawab perlu memastikan semua maklumat bukan rahsia rasmi atau rahsia rasmi di dalam komputer berkenaan telah dikeluarkan dan selamat sebelum menghantar komputer untuk penyelenggaraan

### (c) Keselamatan Pengendalian E-mel Rahsia Rasmi

Perkara-perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan e-mel rahsia rasmi iaitu:

- (i) penyulitan mesti dilakukan ke atas semua e-mel rahsia rasmi yang dihantar, diterima dan disimpan;
- (ii) penerima e-mel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;
- (iii) penerima mesti membuat akuan penerimaan e-mel rahsia rasmi sebaik sahaja menerimanya;
- (iv) 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;
- (v) Jabatan perlu menentukan sistem e-mel rahsia rasmi yang disambungkan kepada internet atau Intranet mesti mempunyai sistem keselamatan yang mencukupi seperti *Firewall* dan *Virtual Private Network*.

## 6.0 TANGGUNGJAWAB PENTADBIR E-MEL DAN INTERNET

Bagi memastikan pengendalian e-mel dan internet agensi beroperasi dengan sempurna dan berkesan, pentadbir sistem ICT adalah bertanggungjawab:

- (a) menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. Pentadbir sistem ICT boleh membekukan akaun

Title: GARIS PANDUAN MENGENAI  
TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK

- pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib;
- (b) menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan pengguna yang lemah dan kemudiannya mencadang dan memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna;
  - (c) menghalang kemasukan maklumat dari laman internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang;
  - (d) menyimpan jejak audit selama sekurang-kurangnya dua (2) bulan di dalam pelayan e-mel berkenaan, tertakluk kepada kemampuan ruang storan, dan tiga (3) tahun di dalam media storan lain;
  - (e) menjalankan pemantauan dan penapisan kandungan fail elektronik dan e-mel secara berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna. Ini bertujuan memastikan pelaksanaannya mematuhi dasar dan tatacara yang ditetapkan;
  - (f) melaksanakan jadual penstoran dan pengarkiban e-mel agensi. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat bernilai;
  - (g) memaklumkan kepada Pegawai Keselamatan ICT (ICTSO) sekiranya mengalami insiden keselamatan seperti pencerobohan sistem, serangan virus atau sebarang masalah kerosakan. Pentadbir sistem ICT hendaklah mengurus dan menangani insiden yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih. ICTSO juga perlu melaporkan setiap insiden kepada GCERT mengikut Pekeliling Am Bil. 1 Tahun 2001 "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; dan
  - (h) melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal perisian dipasang dan berfungsi dengan sempurna.



## 7.0 TANGGUNGJAWAB PENGGUNA

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

- (a) menggunakan akaun atau alamat e-mel yang diperuntukkan oleh jabatan;
- (b) memaklumkan kepada pentadbir email ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;
- (c) menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian dengan merujuk Amalan Baik Keselamatan Kata Laluan di Buku Panduan Keselamatan Maklumat JPN;
- (d) memastikan setiap fail yang dimuat turun bebas dari virus sebelum digunakan;
- (e) bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel di dalam akaun sendiri. Dengan itu, pengguna perlu bertindak bijak, profesional dan berhati-hati apabila berkomunikasi menerusi saluran elektronik;
- (f) berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman internet yang mengandungi unsur-unsur tidak menyenangkan dan memaklumkan perkara ini kepada Pentadbir E-mel dan Internet;
- (g) mengadakan salinan atau penduaan pada media storan kedua elektronik seperti disket dan sebagainya bagi tujuan keselamatan;
- (h) memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan;
- (i) menggunakan kemudahan *password screen saver* atau log keluar apabila hendak meninggalkan komputer;
- (j) memaklumkan kepada Pentadbir E-mel sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan; dan
- (k) memaklumkan kepada pentadbir sistem ICT atau ICTSO sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan ICT.



## 8.0 KELAYAKAN DAN PENGHADAN

Kelayakan capaian ke internet dan E-mel adalah berdasarkan polisi berikut:

- (a) Pegawai JPN adalah terdiri dari Gred 22 dan ke atas. Jika sekiranya pegawai selain dari gred tersebut maka permohonan akan dipertimbangkan mengikut keperluan.
- (b) Tugas harian memerlukan komunikasi dan perhubungan atas talian antara pegawai JPN, pegawai luar dan kontraktor berkenaan urusan rasmi
- (c) Kemudahan capaian dapat meningkatkan produktiviti kerja, penghantaran maklumat yang lebih cepat dan dapat menambah ilmu pengetahuan

Faktor-faktor keselamatan dan ICT berikut perlu diambil kira bagi kebolehan capaian ke internet dan e-mel:

- (a) Segmen VLAN AFIS, Personalization Centre(PERSO), GMPC, ADAM, kaunter dan backoffice SIREN adalah tidak dibenarkan membuat capaian ke internet.
- (b) Semua server urusan JPN seperti server bahagian, SMS dan KPPGate adalah tidak dibenarkan membuat capaian ke internet.
- (c) Segmen yang dibenarkan perlu dikaji dan diperakui keselamatannya oleh satu jawatankuasa teknikal keselamatan ICT yang dipengerusi oleh Pengarah Bahagian Pengurusan Teknologi Maklumat dan Komunikasi (BTM).

## 9.0 KHIDMAT NASIHAT

Sebarang kemusykilan berkaitan dengan Dasar ini dan Garis Panduan Mengenai Tatacara Penggunaan internet dan Mel Elektronik bolehlah dirujuk kepada Bahagian Pengurusan Teknologi Maklumat dan Komunikasi (BTM). Manakala kemusykilan berkaitan dengan Arahan Keselamatan hendaklah dirujuk kepada Bahagian Pertadbiran dan Perkhidmatan (BTK). Permohonan untuk keterangan lanjut mengenai kandungan dokumen ini boleh ditunjukkan kepada:

Jabatan Pendaftaran Negara  
Pengurusan Teknologi Maklumat dan Komunikasi (BTM)  
Aras 4, Lot 2G5, Presint 2  
Pusat Pentadbiran Kerajaan Persekutuan  
62100 PUTRAJAYA.

Tel.: 03-88807000, Faks: 03-88807623 E-mel:  
[administrator@jpn.gov.my](mailto:administrator@jpn.gov.my)



## 10.0 PENUTUP

Garis Panduan ini mengandungi amalan-amalan terbaik penggunaan internet dan mel elektronik yang perlu diikuti oleh semua kakitangan JPN dan akan dikemaskini dari semasa ke semasa selaras dengan arus perkembangan teknologi maklumat dan komunikasi (ICT) dan perundangan. Dokumen ini hendaklah dibaca bersama dengan Dasar Keselamatan Teknologi Maklumat Dan Komunikasi JPN, dokumen *Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS) dan Buku Arahan Keselamatan.

## 11. Rujukan

- 11.1 JPN ICT Security Policy
- 11.2 Buku Panduan Keselamatan Maklumat JPN

