Unit Pemodenan Tadbiran dan

Perancangan Pengurusan Malaysia (MAMPU)

Peraturan Penggunaan Perkhidmatan PCN

Versi 1.6

PCN *Managed Services*

Januari 2020

Isi Kandungan

1.0 Kata Singkatan

BMDF	*Building Main Distribution Frame*
BPGICT	Bahagian Perkhidmatan Gunasama ICT
BYOD	*Bring Your Own Device*
CIDR	*Classless Interdomain Routing Protocol*
DC	Data *Center*
DHCP	*Dynamic Host Configuration Program*
EG	*Electronic Government*
EGW	*External Gateway*
IPv4	*Internet Protocol Version* 4
IPv6	*Internet Protocol Version* 6
GITN	GITN Sdn. Berhad
LAN	*Local Area Network*
MAC	*Medium Access Control*
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
PCN	*Putrajaya Campus Network*
PCN *Switch*	Peralatan Rangkaian yang dimiliki oleh syarikat GITN Sdn. Berhad.
Perkhidmatan PCN	Perkhidmatan PCN secara terurus yang dibekalkan oleh GITN Sdn. Berhad dibawah kontrak MyGov*Net bersama MAMPU.
PMR	*Prime Minister's Residence*
PTR	*Pointer Record*
SDH	*Synchronous Digital Hierarchy*
SLA	*Service Level Agreement*
SSO	*Shared Service Outfit*
TC	*Terminal Closet*
UPS	*Uninterruptible Power Supply*
VIP	*Very Important Person*
VLSM	*Variable Length Subnet Mask*

2.0 Tujuan

Dokumen ini merupakan panduan asas kepada semua pengguna Perkhidmatan Rangkaian Kampus Putrajaya (PCN) untuk menggunakan kemudahan perkhidmatan yang disediakan secara sistematik dan berintegriti. Peraturan penggunaan yang dinyatakan dalam dokumen ini akan membantu agensi-agensi menggunakan sepenuhnya teknologi yang disediakan secara betul dan teratur.

Dokumen ini dirangka dengan mengambil kira piawaian, *standard* dan peraturan-peraturan yang digunakan di Malaysia bagi menyokong inisiatif serta dasar perancangan Kerajaan yang melibatkan Pemusatan Pusat Data, Pembangunan Data Raya, Pengukuhan Keselamatan Siber dan lain-lain.

3.0 Latar Belakang Perkhidmatan Rangkaian Kampus Putrajaya (PCN)

Rangkaian Kampus Putrajaya (PCN) adalah merupakan satu perkhidmatan rangkaian bersepadu dan terurus yang telah dibangunkan mulai tahun 1999. Di awal penubuhannya, PCN dikenali sebagai Putrajaya *Parcel Network* yang diurus oleh Seksyen *Shared Services Outfit* (SSO) di bawah Bahagian Pembangunan Kerajaan Elektronik (BPKE). Skop perkhidmatan Putrajaya *Parcel Network* pada ketika itu hanya meliputi pengurusan infrastruktur rangkaian bagi agensi-agensi Kerajaan di Parcel A dan Parcel B sahaja.

Ekoran dari pertambahan bilangan agensi Kerajaan yang berpindah ke Putrajaya, skop perkhidmatan Putrajaya *Parcel Network* diperluaskan ke agensi-agensi Kerajaan di Parcel C, Parcel D, Parcel E, Presint 2, Presint 3, Presint 4, Presint 5 dan Presint 7. Sejajar dengan perluasan skop yang pesat ini,Putrajaya *Parcel Network* diubah nama kepada Rangkaian Kampus Putrajaya (PCN). Pengurusan PCN juga tidak lagi di bawah SSO tetapi diletakkan di bawah BPGICT yang ditubuhkan pada Ogos 2009.

PCN telah melalui fasa penukaran Teknologi yang pertama secara sepenuhnya (PCN *Overhaul*) pada 2008 iaitu penukaran Teknologi ATM (*Asynchronous Transfer Mode*) kepada Teknologi GE (*Gigabit Ethernet*). Penukaran ini dibuat bagi mempertingkatkan keupayaan rangkaian sejajar dengan teknologi terkini pada masa tersebut.

Sehingga kini, sebanyak 80 agensi meliputi 22 kementerian, 4 PDSA, lebih kurang 70 Pusat Data / Bilik *Server* Agensi dengan lebih 50,000 pengguna menggunakan Perkhidmatan PCN untuk kemudahan capaian ke Internet, capaian kepada intranet dan komunikasi elektronik antara agensi Kerajaan.

Pada 2014, PCN telah dimasukkan ke dalam perkhidmatan MyGov*Net di bawah kategori "*Optional Services*" mengikut kelulusan Kabinet di mana pecahan perkhidmatan dibahagikan kepada dua fasa:

a. Fasa 1: Perkhidmatan penyelenggaraan PCN secara komprehensif bermula dari Januari 2014 sehingga Disember 2017 dimana semua peralatan rangkaian adalah milik Kerajaan.

b. Fasa 2: Bermula Januari 2018 sehingga Disember 2022, perkhidmatan rangkaian PCN dilaksanakan secara PCN *Managed Services* di mana kesemua peralatan PCN di bawah skop fasa 1 telah dipindah milik kepada syarikat melalui kaedah tukaran barangan dan perkhidmatan (*barter trade*).

Sehubungan dengan itu, satu tatacara peraturan penggunaan perkhidmatan perlu dibangunkan untuk memberi panduan kepada agensi menggunakan Perkhidmatan PCN secara teratur dan betul.

4.0 Skop Peraturan Penggunaan Perkhidmatan PCN

Dokumen ini terpakai kepada semua agensi Kerajaan di Putrajaya yang menggunakan Perkhidmatan PCN di bawah skop PCN *Managed Services*. Senarai agensi Kerajaan yang dibawah skop ini adalah seperti **Lampiran A.**

Peraturan penggunaan Perkhidmatan PCN ini adalah terpakai kepada semua pengguna Perkhidmatan PCN sama ada penjawat awam, syarikat penyelenggara bangunan atau pembekal-pembekal yang berurusan dengan agensi.

Dokumen ini adalah peraturan penggunaan yang menentukan bagaimana Rangkaian PCN diurus dan dilindungi yang perlu diambil maklum dan dipatuhi oleh agensi.

5.0 Pematuhan

Dokumen ini hendaklah dipatuhi sepenuhnya bagi mengelakkan sebarang bentuk ketidakpatuhan ke atas peraturan yang boleh mengancam keselamatan Perkhidmatan PCN. Dokumen ini perlu dibaca bersama pekeliling dan dasar keselamatan agensi yang berkuatkuasa.

MAMPU berhak untuk menamat / menyekat Perkhidmatan PCN kepada agensi sekiranya peraturan penggunaan Perkhidmatan PCN ini tidak dipatuhi.

6.0 Penyataaan Peraturan Penggunaan Perkhidmatan PCN

Dokumen ini telah dirangka dengan mengambil kira hala-tuju serta dasar perancangan Kerajaan seperti Pemusatan Pusat Data, Pembangunan Data Raya, Pengukuhan Keselamatan Siber dan lain-lain. Peraturan ini merangkumi elemen-elemen seperti berikut:

6.1	Capaian Rangkaian
6.2	Penggunaan Internet
6.3	Alamat IP (IP *Addressing*)
6.4	DNS *Services*
6.5	Peralatan Keselamatan dan Peralatan Pengukuran Keupayaan
6.6	Pelayan, Komputer Peribadi, *Notebook* dan peralatan BYOD
6.7	Bilik BMDF dan Bilik *Telco*
6.8	Sistem Pengkabelan
6.9	*Leased Lines* dan VPN
6.10	*Switch* LAN milik Agensi
6.11	*Wireless Access Points* (AP) Agensi

6.1 Capaian Rangkaian

a) Semua pengguna Perkhidmatan PCN hendaklah penguna yang sah dan berdaftar (*authenticated users*). Pengguna yang sah adalah pengguna yang telah didaftar di dalam *directory services* agensi masing-masing.

b) Sebelum pengguna dibolehkan membuat capaian pada rangkaian, pengguna dikehendaki memasukkan ID dan kata laluan untuk semakan pada *directory services*.

c) Capaian rangkaian PCN boleh dibuat melalui capaian berwayar, capaian tanpa wayar dan capaian secara *remote.*

d) Capaian berwayar dalam Perkhidmatan PCN adalah capaian yang dibuat melalui sambungan UTP dan Fiber Optik ke LAN *Switch* sahaja.

e) Capaian tanpa wayar di PCN adalah capaian yang berdasarkan kepada WiFi *standard* IEEE 802.11 sahaja.

f) Capaian secara *remote* seperti SSL VPN, adalah capaian yang dibuat dari luar PCN melalui *Remote Access Controller*. Capaian ini hanya dibenarkan setelah ID dan kata laluan disahkan. Permohonan ID and kata laluan baru boleh dibuat melalui meja bantuan MyGov*Net.

g) Kesemua peralatan yang menggunakan Rangkaian Perkhidmatan PCN perlu menyeragamkan *Network Time Protocol* (NTP). Agensi dikehendaki merujuk kepada sumber *Network Time Protocol* (NTP) yang disediakan oleh PCN bagi penyeragaman waktu bagi Pelayan, Aplikasi dan peralatan rangkaian milik agensi. Semua peralatan yang menggunakan rangkaian PCN hendaklah mengikut *Network Time Protocol* (NTP) ditetapkan oleh PCN mengikut piawaian SIRIM.

6.2 Penggunaan Internet

a) Kemudahan Internet hendaklah digunakan bagi tujuan tugasan rasmi. Laman yang dilayari hendaklah berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan.

b) Pengguna dilarang melakukan sebarang aktiviti yang boleh memberi ancaman keselamatan siber kepada Internet PCN.

c) Semua data sensitif dan fail-fail sulit atau maklumat terperingkat yang dipindahkan menerusi talian Internet haruslah mendapatkan tandatangan digital yang dikeluarkan oleh pihak berkuasa perakuan tempatan yang ditauliahkan oleh Kerajaan Malaysia iaitu Pihak Berkuasa Persijilan (*Certification Authority*) terlebih dahulu.

d) Pengguna adalah dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet PCN seperti:

   i. Memuat naik, memuat turun dan menyimpan material yang mengandungi bahan-bahan yang berunsur lucah.

   ii. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen.

   iii. Memuat turun, membuat instalasi dan mengguna perisian percuma yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian PCN.

   iv. Memuat naik atau memuat turun, menghantar dan menyimpan fail-fail bersaiz besar melebihi 1Gb yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer. Bagi memuat naik, memuat turun, dan menghantar fail-fail yang melebihi 1Gb, pengguna perlulah mendapatkan kelulusan daripada pihak MAMPU dan dibuat selepas waktu puncak.

v. Menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang penyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan.

vi. Menggunakan aplikasi-aplikasi *streaming* seperti *Online Radio*, Netflix, Kodi dan sebagainya kerana ia boleh mengganggu prestasi rangkaian internet PCN kecuali untuk tugasan rasmi dan mendapat kelulusan daripada pihak MAMPU.

vii. Menggunakan kemudahan internet PCN ini untuk tujuan perniagaan dan berpolitik yang berbentuk peribadi.

viii. Menggunakan Internet PCN untuk tujuan melanggar undang-undang dan regulasi Malaysia ataupun mana-mana negara lain.

6.3 Alamat IP *(IP Addressing)*

a) Blok IP dalam PCN adalah di bawah kawalan Perkhidmatan PCN. Bagi pembangunan rangkaian dalaman agensi, pihak agensi tidak dibenarkan untuk menggunapakai alamat IP yang konflik dengan blok IP PCN. Agensi dibenarkan menggunakan IP *private* IPv4 seperti 192.168.x.x/16 atau IPv6 seperti fc00::/7 dengan syarat IP tersebut tidak di *advertise*kan ke dalam Rangkaian PCN.

b) Agensi perlu menyediakan perkhidmatan DHCP sendiri bagi mengelakkan berlaku konflik alamat IP bagi peralatan dalam rangkaian agensi. Agensi perlu menetapkan *exclusion* khas daripada DHCP *Scope* bagi pengendalian pelayan – pelayan aplikasi yang menggunakan statik IP.

c) Alamat IP bagi peralatan WiFi diberikan secara automatik oleh DHCP yang disediakan oleh Perkhidmatan PCN. Polisi keselamatan *(allow* / *deny),* bagi capaian ke aplikasi / pelayan / peralatan agensi dari alamat IP DHCP WiFi PCN adalah tanggungjawab agensi.

d) Penggunaan *Proxy* IP, *Reverse Proxy* IP atau IP NAT bagi rangkaian PCN perlu dimaklumkan kepada MAMPU.

e) Bagi mengoptimakan penggunaan IP dan pengagihan IP, agensi harus mengaplikasikan teknik VLSM atau CIDR.

6.4 DNS *Services*

a) Agensi perlu menyediakan (DNS) untuk pengenalan nama *domain*, *Resolve* dan *Queries. Server* DNS boleh dibangunkan secara luaran, dalaman atau kedua-keduanya.

b) DNS dalaman yang dibangunkan oleh agensi adalah *'authoritative'* kepada semua rekod-rekod zon dibawahnya dan mestilah dikonfigurasi sebagai *Master* DNS.

c) Bagi tujuan pendaftaran *domain* baharu, agensi perlu memberi maklumat seperti berikut melalui sistem MyGovOSF:

   i) Nama *domain*;
   ii) Maklumat zon;
   iii) Alamat IP; dan
   iv) Maklumat Rekod Sumber (*Resource Record Information*)

d) Untuk tujuan penambahan , pengemaskinian dan penghapusan rekod DNS, agensi perlu memberi maklumat seperti berikut melalui sistem MyGovOSF:

   i) Nama *domain*;
   ii) Maklumat zon;
   iii) Alamat IP; dan
   iv) Maklumat Rekod Sumber (*Resource Record Information*)

e) Agensi dikehendaki menamakan *sub domain* rekod bagi zon mereka dengan nama yang bersesuaian dan berkaitan dengan identity zon tersebut. Nama *sub domain* rekod zon yang tidak menggambarkan identiti rekod adalah dilarang kerana isu keselamatan.

f) Agensi dikehendaki menetapkan rekod sumber *(resource record)* PTR bagi rekod e-mel seperti rekod MX dan rekod A/AAAA untuk carian peta balikan (*reverse map-lookup*).

g) Bagi memastikan ketersediaan perkhidmatan DNS, agensi dikehendaki membenarkan maklumat zon disalin ke *Secondary* DNS *Server* yang disediakan oleh Perkhidmatan PCN. Segala *parameter* berkaitan konfigurasi DNS perlulah dikonfigur pada *Master* DNS bagi membolehkan *autotransfer* ke *secondary* berlaku.

h) Bagi DNS agensi yang memerlukan DNS *forwarder, forwarder server* tersebut mestilah menggunakan DNS *Server* yang disediakan oleh Perkhidmatan PCN dalam MyGovNet / PCN.

6.5 Peralatan Keselamatan dan Peralatan Pengukuran Prestasi Rangkaian

a) VLAN agensi (*non fabric*) yang merangkumi VLAN pengguna dan VLAN pusat data mesti dilindungi oleh peranti keselamatan seperti IPS dan *Firewall* milik agensi.

b) Agensi bertanggungjawab untuk menjaga dan menyelenggara (*patches*, *signature update* dll) peranti keselamatan seperti IPS, *Firewall,* Pelayan Proksi, *Anti-Virus Server* dan lain-lain.

c) Agensi bertanggungjawab untuk menjaga dan menyelenggara (*patches, signature update* dll) peranti prestasi *(performance devices)* atau pembentuk paket *(packet shaper)*.

d) Semua aktiviti atau insiden yang berkaitan dengan keselamatan pada sistem yang kritikal hendaklah dilog dan dijejak audit *(audit trails)* dengan mengikut perkeliling dan dasar keselamatan ICT yang sedang berkuatkuasa.

e) Audit keselamatan mesti dilaksanakan secara berkala. Kekurangan atau kelemahan *(Vulnerabilities)* yang ditemui perlu dianalisis dan diambil langkah-langkah pembetulan. Antara insiden keselamatan yang perlu diaudit adalah seperti berikut:

   i. Penyebaran Virus;
   ii. Serangan Imbasan *Port*;
   iii. Bukti akses tanpa izin ke akaun Sah; dan
   iv. *Abnormally* yang tidak berkaitan dengan *a*plikasi tertentu pada *host.*

6.6 Pelayan, Komputer Peribadi, *Notebook* dan Peralatan BYOD.

6.6.1 Ciri-ciri Keselamatan

a) Pelayan, Komputer Peribadi (PC) *Notebook* dan peralatan BYOD seperti *mobile phone, tablet* dan lain-lain peralatan yang berkaitan mestilah bebas dari Virus*, Trojan, Malware* dan semua *Malicious Code* sebelum ia disambungkan ke rangkaian PCN.

b) Agensi hendaklah memastikan peralatan seperti di para (a) memiliki Sistem Pengoperasian, perisian aplikasi yang terkini serta dikemaskini mengikut keperluan dan sentiasa berada di dalam tempoh masa *'product support'.*

c) Agensi hendaklah mengambil tindakan untuk memastikan semua peralatan seperti di para (a) bebas daripada ancaman siber.

d) Agensi hendaklah memastikan peralatan seperti di para (a) dipasang dengan perisian anti-virus.

e) Perisian antivirus yang dipasang mestilah berupaya mengesan dan bertindakbalas pada sebarang *abnormality* atau ancaman siber.

f) Agensi hendaklah memastikan antivirus yang dipasang:
i) Perisian antivirus mempunyai lesen yang sah dan asli.
ii) Sentiasa dikemaskini dengan virus *attack signatures database* terkini.

g) "*Health Status*" bagi setiap peralatan akan dipantau oleh Perkhidmatan PCN.

h) Sebarang *malicious activity* yang berpunca dari peralatan tersebut akan dikuarantin dan mungkin terhalang daripada menggunakan rangkaian.

6.6.2 BYOD dan IOT

a) Pengguna BYOD boleh menggunakan rangkaian PCN sama ada sebagai agensi dalam PCN ataupun sebagai pelawat.

b) Pengguna BYOD bagi profil staf perlu mengaktifkan *authentication* 802.1x sebelum menggunakan rangkaian PCN dengan merujuk kepada pentadbir IT Agensi masing-masing dan panduan pengguna boleh didapati di www.mygovnet.gov.my.

c) Dua kategori profil bagi pengguna staf dalam PCN iaitu;

i. Profil kakitangan VIP – Gred 54 dan ke atas/ Jawatan Timbalan Pengarah/ Timbalan Setiausaha dan ke atas.

ii. Profil kakitangan biasa – Gred 52 dan ke bawah / Ketua Penolong Pengarah Kanan/ Ketua Penolong Setiausaha Bahagian

6.6.3 *Authentication*

a) *Authentication* bagi perkhidmatan rangkaian PCN adalah berdasarkan IEEE 802.1x yang juga melibatkan pengguna *wired*.

b) Agensi perlu membuat pendaftaran MAC *Address* bagi peralatan IoT yang menggunakan Perkhidmatan PCN.

c) Agensi perlu mewujudkan kategori kumpulan (*group category)* Kontraktor pada *Authentcation Server* agensi seperti *Active Directory*. Polisi khas untuk Kontraktor perlu dilaksanakan sebagai kawalan keselamatan capaian dan penggunaan Rangkaian.

d) Bagi agensi yang tidak memiliki *Authentication Server*, kategori kumpulan Kontraktor ini akan diwujudkan di *Authentication Server* Perkhidmatan PCN. Permohonan perkhidmatan ini boleh dibuat menerusi Sistem Permohonan Perkhidmatan PCN.

d) Penukaran *Password* bagi *authentication* IEEE 802.1x yang disediakan oleh Perkhidmatan PCN boleh dibuat melalui Portal www.mygovnet.gov.my.

e) Pelawat boleh menggunakan dua kaedah *Web Authentication* iaitu;
   i) *Self Registration*
   ii) *Facebook social login*

f) Pengguna hendaklah membuat semakan melalui meja bantuan MyGov*Net bagi peralatan-peralatan yang tidak menyokong teknologi IEEE 802.1x sekiranya perlu menggunakan Perkhidmatan PCN.

g) Pelawat hanya diperuntuk tempoh masa satu jam bagi setiap *active session* semasa menggunakan Rangkaian PCN.

h) Peralatan BYOD yang hilang hendaklah dilaporkan ke meja bantuan Perkhidmatan PCN bagi membolehkan BYOD tersebut dikuarantin.

i) Peralatan BYOD yang dijumpai perlu dilaporkan semula ke meja bantuan bagi tujuan pengaktifan.

6.7 Bilik BMDF dan Bilik Telco

a) *Switch* PCN yang ditempatkan di dalam bilik BMDF dan bilik Telco adalah hak milik Perkhidmatan PCN dan agensi tidak dibenarkan mengalihkan atau merubah posisi.

b) Agensi tidak dibenarkan membuat sebarang sambungan kabel ke *switch* PCN tanpa kebenaran Perkhidmatan PCN.

c) Semua permohonan perkhidmatan yang melibatkan *switch* PCN seperti pertambahan kabel / *patch* panel ataupun pengguna hendaklah melalui Sistem Permohonan Perkhidmatan PCN.

d) Pihak agensi dan Penyelenggara Bangunan hendaklah bertanggungjawab dalam memastikan keselamatan dan kebersihan persekitaran bilik BMDF dan Telco.

e) Penyelenggara bangunan hendaklah membuat penyelengaraan berkala melibatkan kerja-kerja Mekanikal & Elektrikal terhadap kesemua bilik BMDF dan bilik Telco.

6.8 Sistem Pengkabelan

a) Kabel UTP *horizontal* adalah di bawah tanggungjawab agensi.

b) *Vertical Cable* dan *interbuilding fiber optic* adalah di bawah tanggungjawab Perkhidmatan PCN.

c) Sekiranya agensi perlu membuat pemasangan *horizontal cable* UTP ianya hendaklah mengikut piawaian Sistem Pengkabelan *Ethernet* EIA/TIA dengan spesifikasi 586B minimum Cat 6. Agensi hendaklah memastikan susun atur kabel sentiasa berada dalam keadaan kemas.

d) Agensi hendaklah memastikan keselamatan sistem pengkabelan bangunan.

6.9 *Leased Lines* dan VPN

a) Agensi dilarang memasang sebarang bentuk *connectivity Leased Lines* dan VPN. Sekiranya ada keperluan, agensi hendaklah memohon secara rasmi kepada MAMPU. Agensi hendaklah mengasingkan rangkaian yang memerlukan capaian tersendiri ke internet dari rangkaian PCN.

b) Syarikat GITN Sdn Bhd adalah pembekal tunggal perkhidmatan Internet dan Intranet MyGov*Net bagi agensi-agensi dibawah skop PCN *Managed Services.*

c) Bagi Capaian Jauh VPN *(Remote Access VPN), termination* VPN bagi agensi mestilah berlaku di *Gateway PCN* sama ada di Pusat Data BPGICT di Parcel B, Blok B8, Level -2 atau Pusat Data BPGICT di Blok 2M11. Setiap Capaian Jauh VPN bagi PCN adalah dikawal dan dipantau.

d) Sekiranya agensi memerlukan capaian jauh VPN terus di pusat data agensi, kelulusan daripada pihak MAMPU adalah diperlukan. Penggunaan VPN dan *Remote Access* di bawah seliaan agensi mesti mematuhi peraturan ICT dan DKICT agensi.

e) Syarikat GITN akan menyediakan *Remote Access VPN termination* bagi kesemua VPN yang memasuki PCN secara *Remote*. Kata laluan, Password, *access list* dan alamat IP bagi *Remote Access* VPN ini disediakan oleh Syarikat GITN.

6.10 *Switch* LAN milik Agensi

a) Agensi tidak dibenarkan memasang dan menyambung sebarang *third-party Switch* LAN kepada *Switch* LAN yang dibekalkan oleh Perkhidmatan PCN sama ada di dalam TC *Room* atau di *port* I/O pengguna.

b) Pemasangan *switch* LAN untuk tujuan khas terutamanya di dalam pusat data seperti *Secured Zone LAN Switch* atau *DMZ LAN Switch* dibenarkan tetapi rekabentuk *connectivity* bagi *switch* tersebut mestilah dimaklumkan kepada Perkhidmatan PCN.

c) *Switch* LAN agensi tidak akan dipantau atau diselenggara oleh Perkhidmatan PCN.

d) Keselamatan *Switch* LAN agensi adalah tanggungjawab agensi.

e) Prefix 10.18.x.x. dan 10.88.x.x adalah alamat IP yang digunakan khusus untuk peralatan Perkhidmatan PCN. Agensi tidak dibenarkan menggunakan prefix tersebut.

f) Semua *Switch* LAN milik agensi hendaklah dilabelkan.

6.11 *Wireless Access Points* (AP) Agensi

a) Perkhidmatan PCN WiFi telah disediakan oleh MAMPU yang meliputi keseluruhan ruang pejabat agensi yang terlibat. Agensi tersebut dilarang mewujudkan zon WiFi sendiri.

b) Kelulusan rasmi dari pihak MAMPU hendaklah diperoleh sekiranya agensi ingin mewujudkan zon WiFi sendiri di lokasi agensi yang telah berada dalam liputan WiFi PCN dengan mengambilkira perkara seperti di bawah:

   i. Enkripsi yang mematuhi sekurang-kurangnya WPA-2

   ii. SSID yang tidak menyerupai SSID WiFi PCN

c) Pemasangan peralatan zon WiFi Agensi tidak boleh menggunakan Prefix 10.18.x.x dan 10.88.x.x kerana IP tersebut khusus untuk peralatan Perkhidmatan PCN.

d) MAMPU hendaklah dimaklumkan secara rasmi sekiranya agensi perlu membuat pemasangan peralatan keselamatan tambahan yang memberi impak kepada Perkhidmatan WiFi PCN. Sebagai contoh, *jammer*, WIPS, *Rogue AP detection* dan *Firewall Policy.*