KERAJAAN MALAYSIA

SURAT ARAHAN KETUA PENGARAH JABATAN DIGITAL NEGARA BILANGAN 5 TAHUN 2025

GARIS PANDUAN PEMBANGUNAN DAN PENGOPERASIAN RANGKAIAN KAWASAN SETEMPAT (*LOCAL AREA NETWORK*, LAN) SEKTOR AWAM

JABATAN DIGITAL NEGARA
KEMENTERIAN DIGITAL

KANDUNGAN

KETUA PENGARAH
JABATAN DIGITAL NEGARA
Aras 6, Bangunan MKN Embassy Techzone
Blok B, No. 3200 Jalan Teknokrat 2
63000 Cyberjaya, Sepang
SELANGOR DARUL EHSAN
MALAYSIA

Telefon : 603-88723010
Laman Web : www.jdn.gov.my

Rujukan : JDN.100-1/5/1(3)

Tarikh : 2 September 2025

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

SURAT ARAHAN KETUA PENGARAH JABATAN DIGITAL NEGARA BILANGAN 5 TAHUN 2025

GARIS PANDUAN PEMBANGUNAN DAN PENGOPERASIAN RANGKAIAN KAWASAN SETEMPAT (*LOCAL AREA NETWORK* (LAN)) SEKTOR AWAM

TUJUAN

1. Surat Arahan ini bertujuan untuk memaklumkan mengenai Garis Panduan Pembangunan dan Pengoperasian Rangkaian Kawasan Setempat (*Local Area Network* (LAN)) Sektor Awam bagi membantu agensi di Sektor Awam membuat perancangan, pengoperasian, pengurusan, penyelenggaraan dan pemantauan LAN di agensi masing-masing.

LATAR BELAKANG

2. Kemajuan pesat dalam bidang teknologi maklumat dan komunikasi (ICT) telah meningkatkan keperluan untuk penyediaan infrastruktur rangkaian yang cekap, selamat dan terurus dengan baik dalam menjayakan agenda pendigitalan sektor awam. Infrastruktur LAN merupakan komponen asas dan penting dalam menyokong penyampaian perkhidmatan digital, pelaksanaan aplikasi kerajaan, komunikasi dalaman serta integrasi dengan perkhidmatan berasaskan pengkomputeran awan. Tanpa sistem rangkaian yang stabil, selamat dan dikawal selia secara menyeluruh, keupayaan agensi untuk beroperasi secara digital akan terjejas, sekali gus meningkatkan risiko terhadap keselamatan siber dan menjejaskan kesinambungan penyampaian perkhidmatan kerajaan.

3. Peningkatan kebergantungan terhadap LAN dan capaian secara atas talian telah mendedahkan sistem kepada pelbagai risiko keselamatan maklumat seperti kebocoran data, serangan siber dan penyalahgunaan akses. Sehubungan dengan itu, pembangunan dan pengoperasian LAN perlu dirangka dan dikendalikan menerusi garis panduan yang mematuhi polisi keselamatan siber semasa serta selaras dengan dasar dan akta yang berkuat kuasa.

4. Terdapat cabaran dalam pelaksanaan ini apabila sebahagian dasar atau garis panduan terdahulu telah menjadi tidak sah atau kurang relevan berikutan perubahan pantas landskap teknologi, perundangan dan ancaman siber. Justeru itu, keperluan untuk menyelaraskan semula dasar dan garis panduan adalah penting agar selari dengan dokumen dan perubahan terkini.

KEPERLUAN/RASIONAL

5. Agensi perlu melaksanakan penilaian keperluan lebih berkesan secara menyeluruh meliputi aspek pembangunan, pengoperasian, teknologi, kaedah, serta jenis perkhidmatan yang akan disokong oleh rangkaian ICT. Pendekatan ini penting bagi memastikan pembangunan dan pengoperasian LAN adalah berstruktur, selamat dan berdaya tahan.

6. Rangkaian ICT yang kukuh dan mantap perlu dibangunkan berasaskan standard reka bentuk dan konfigurasi yang seragam, selaras dengan dasar ICT semasa serta mematuhi polisi keselamatan siber. Ia juga hendaklah menyokong kelancaran operasi harian agensi, di samping meningkatkan prestasi sistem dan memperkukuh kualiti penyampaian perkhidmatan kerajaan.

7. Pendekatan ini juga membantu memperkukuh keselamatan siber dengan mengurangkan pendedahan kepada ancaman yang boleh menjejaskan kelancaran operasi kerajaan, selain memastikan pengurusan rangkaian berterusan dapat dijalankan secara lebih berkesan. Di samping itu, pengurusan rangkaian yang cekap turut membolehkan pengoptimuman kos operasi ICT, menjadikan pelaburan dalam infrastruktur digital lebih lestari dan memberi nilai tambah kepada kerajaan serta rakyat.

STRUKTUR TADBIR URUS

8. Tadbir Urus Pembangunan dan Pengoperasian LAN di agensi adalah seperti di **Bab 2: Tadbir Urus** dalam garis panduan ini.

PEMAKAIAN

9. Surat Arahan ini terpakai kepada semua agensi Perkhidmatan Awam Persekutuan. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Arahan ini dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun dan Pihak Berkuasa Tempatan (PBT).

TARIKH KUAT KUASA

10. Surat Arahan ini berkuat kuasa serta-merta mulai daripada tarikh ia dikeluarkan.

PERTANYAAN

11. Sebarang pertanyaan mengenai Surat Arahan ini boleh dirujuk kepada:

Pengarah
Bahagian Perundingan Digital
Jabatan Digital Negara
Kementerian Digital
Bangunan MKN Embassy Techzone
Blok B, No. 3200, Jalan Teknokrat 2
63000 Cyberjaya
SELANGOR DARUL EHSAN
No. Telefon : 03-8000 8000
E-mel : nmu@jdn.gov.my
Laman Web : https://www.jdn.gov.my

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"

Saya yang menjalankan amanah,

(TS. NIK ZALBIHA BINTI NIK MAT)

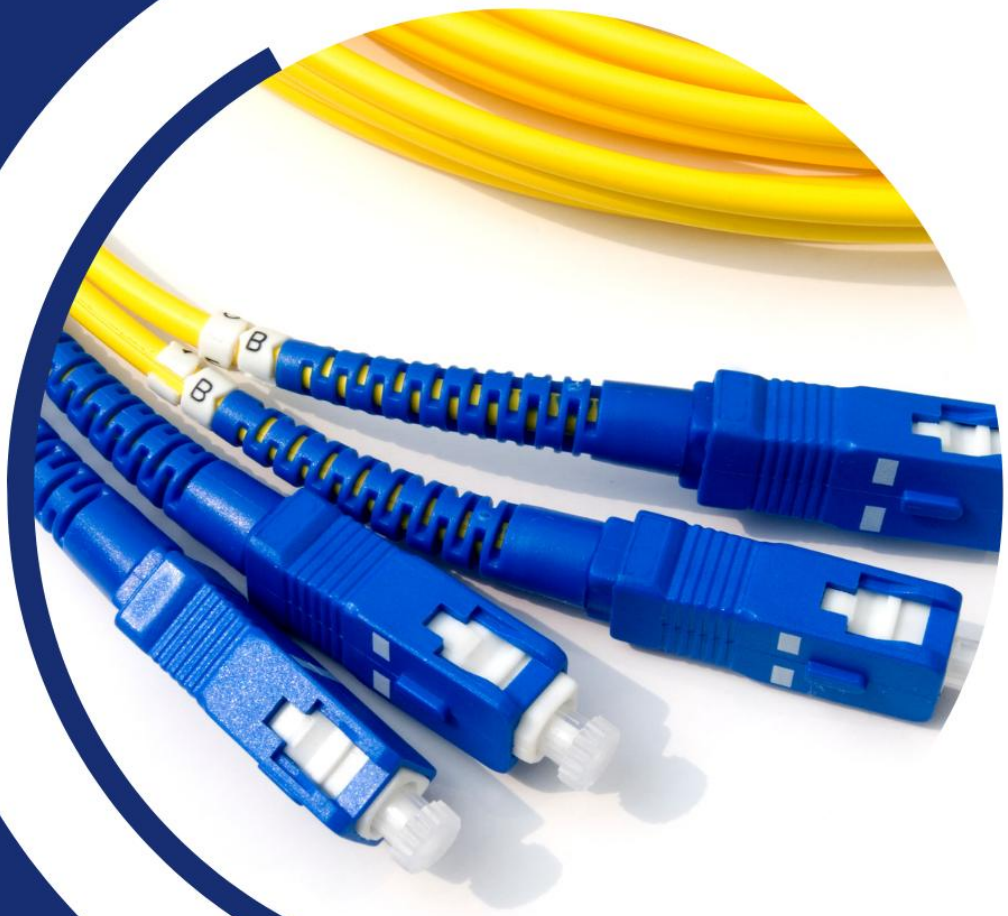
SENARAI LAMPIRAN

LAMPIRAN A
Surat Arahan Ketua Pengarah Jabatan Digital Negara
Bilangan 5 Tahun 2025

GARIS PANDUAN PEMBANGUNAN DAN PENGOPERASIAN RANGKAIAN KAWASAN SETEMPAT (*LOCAL AREA NETWORK* (LAN)) SEKTOR AWAM

JABATAN DIGITAL NEGARA
KEMENTERIAN DIGITAL

KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA



GARIS PANDUAN

PEMBANGUNAN DAN PENGOPERASIAN RANGKAIAN KAWASAN SETEMPAT (LAN) SEKTOR AWAM

KANDUNGAN

PERKARA **MUKA SURAT**

SENARAI RAJAH

SENARAI JADUAL

AKRONIM

AKRONIM	PENERANGAN
4G	*Fourth-generation of cellular network technology*
5G	*Fifth-generation of cellular network technology*
AAA	*Authentication, Authorization and Accounting*
ACL	*Access Control Lists*
R&D	Penyelidikan dan Pembangunan
AD	*Active Directory*
AI	*Artificial Intelligence*/Kecerdasan Buatan
AP	Titik Capaian/*Access Point*
APT	*Advanced Persistent Threat*
AS	*Access Switch*
ATP	*Advanced Threat Protection*
BMT	*Bandwidth Management Tool*
BYOD	*Bring Your Own Device*
CCTV	*Closed Circuit Television*
CF	*Content Filtering*
CDO	*Chief Digital Officer*/Ketua Pegawai Digital
CIA	*Confidentiality, Integrity and Availability*
CMDB	*Configuration Management Database*
CPU	*CentralProcessing Unit*
CS	*Core Switch*
DAI	*Dynamic ARP Inspection*
dBm	*Decibel-Milliwatts*
DHCP	*Dynamic Host Configuration Protocol*
DKICT	Dasar Keselamatan ICT
DMZ	*Demilitarized Zone*
DNS	Sistem Nama Domain/*Domain Name System*
DS	*Distribution Switch*
EAL	*Evaluation Assurance Level*
EOL	*End of Life*
EOS	*End of Sale*

AKRONIM	PENERANGAN
FCAPS	*Fault, Configuration, Accounting, Performance and Security*
FAT	Ujian Penerimaan Akhir/*Final Acceptance Test*
FQDN	*Senarai Kemas Kini Nama Domain/Fully Qualified Domain Name*
GB	*Gigabyte*
GNS-3	*Graphical Network Simulator-3*
Gbps	*Gigabits per second*
HA	*High Availability*
HTTPS	*Hypertext Transfer Protocol Secure*
ICT	*Information and Communications Technology*
IAM	*Identity Access Management*
IDM	*Identity Management*
IDS	Sistem Pengesanan Pencerobohan/ *Intrusion Detection System*
IEEE	*Institute of Electrical and Electronics Engineers (IEEE)*
IoT	Internet Benda/*Internet of Things*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
IPS	Sistem Penghalang Pencerobohan/*Intrusion Prevention System*
IR 4.0	Revolusi Industri 4.0
ISMP	Pelan Pengurusan Keselamatan Maklumat
ISMS	Information Security Management System
ISO	Organisasi Piawaian Antarabangsa
ISP	Pembekal Khidmat Internet/ *Internet Service Provider*
JDN	Jabatan Digital Negara
JPICT	Jawatankuasa Pemandu ICT Sektor Awam
KPI	*Key Performance Indicator*
LACP	*Link Aggregation Control Protocol*
LAN	Rangkaian Kawasan Setempat/ *Local Area Network*
LDAP	*Lightweight Directory Access Protocol*

AKRONIM	PENERANGAN
Mbps	*Megabits per second*
MDF	*Main Distribution Frame Room*
MAC	*Media Access Control*
MFA	*Multi Factor Authentication*
NAC	Kawalan Akses Rangkaian/*Network Access Control*
NDLC	Kitar Hayat Pembangunan Rangkaian/ *Network Development Life Cycle*
NACSA	Agensi Keselamatan Siber Negara/ *National Cyber Security Agency*
NGFW	Tembok Keselamatan Generasi Masa Hadapan/ *Next Generation Firewall*
NMS	Sistem Pengurusan Rangkaian/*Network Management System*
NOC	*Network Operations Center*
NTP	*Network Time Protocol*
OM4/OM5	*Optical Multimode (OM)* – tahap 4/5
OS2	*Optical Singlemode (OS)* – tahap *2*
OSPF	*Open Shortest Path First*
PABX	*Private Automatic Branch Exchange*
PAT	Ujian Penerimaan Sementara/*Provisional Acceptance Test*
PBT	Pihak Berkuasa Tempatan
PCN	Putrajaya *Campus Network*
PDSA	Pusat Data Sektor Awam
PKS	Polisi Keselamatan Siber
PoC	*Proof of Concept*
PoV	*Proof of Value*
PPrISA	Panduan Pengurusan Projek ICT Sektor Awam
PSP	Pelan Strategik Pendigitalan
PSPSA	Pelan Strategik Pendigitalan Sektor Awam
QoS	*Quality of Service*

AKRONIM	PENERANGAN
RF	Frekuensi Radio/*Radio Frequency*
RFI	*Request For Information*
RSSI	*Received Signal Strength Indicator*
SDF	*Subscriber Distribution Frame*
SDN	*Software Defined Network*
SIEM	*Security Information and Event Management*
SIRIM	Institut Piawaian dan Penyelidikan Perindustrian Malaysia
SLA	*Service Level Agreement*
SLG	*Service Level Guarantees*
SSH	*Secure Shell/Secure Socket Shell*
SOC	*Security Operations Center*
SOP	Prosedur Operasi Standard/*Standard Operating Procedure*
SNMP	*Simple Network Management Protocol*
STP	*Spanning Tree Protocol*
TCR	*Telecommunication Closet Room*
UAT	Ujian Penerimaan Pengguna/*User Acceptance Test*
URL	*Uniform Resource Locator*
UTP	*Unshielded Twisted Pair*
VLAN	*Virtual Local Area Network*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
WAN	Rangkaian Kawasan Luas/*Wide Area Network*
WIPS	Sistem Penghalang Pencerobohan Wayarles/ *Wireless Intrusion Prevention System*
WI-FI	*Wireless Fidelity*
WLAN	Wayarles LAN
WLC	Wayarles LAN *Controller*
WPA	*WiFi Protected Access*

TAKRIFAN

Bagi maksud pemakaian Surat Arahan Ketua Pengarah Jabatan Digital Negara Bilangan 5 Tahun 2025 Garis Panduan Pembangunan dan Pengoperasian Rangkaian Kawasan Setempat (*Local Area Network*, LAN) Sektor Awam, takrifan yang berikut diguna pakai:

1.	Agensi Sektor Awam	Agensi kerajaan merujuk kepada Kementerian atau Jabatan atau agensi dalam Sektor Awam.
2.	Infrastruktur ICT	Infrastruktur ICT melibatkan perkakasan ICT, perisian ICT dan rangkaian ICT.
3.	Infrastruktur sokongan	Infrastruktur sokongan merujuk kepada kemudahan seperti bekalan elektrik, penyaman udara, alat penggera, CCTV, keselamatan fizikal untuk menempatkan perkakasan ICT terutamanya di bilik pelayan.
4.	Pembekal	Syarikat yang membekal atau menyelenggara atau memberikan perkhidmatan peralatan rangkaian di agensi.
5.	Pentadbir Rangkaian	Pegawai Teknologi Maklumat atau Pegawai dengan huraian kerja (*job description*) untuk mentadbir rangkaian di agensi.
6.	Perkhidmatan MyGov*Net	Rangkaian Telekomunikasi Bersepadu Kerajaan yang diuruskan secara terpusat oleh JDN.

7.	*Port* rangkaian	Soket pada peranti rangkaian atau mana-mana perkakasan komputer sama ada di dinding atau lantai yang membenarkan sambungan kabel daripada peranti lain bagi tujuan komunikasi.
8.	Pusat Data Sektor Awam (PDSA)	Fasiliti pusat data dan infrastruktur ICT yang disediakan oleh JDN.
9.	Rangkaian Kawasan Luas (WAN)	Sistem jaringan rangkaian yang merentasi lokasi yang sangat luas dan boleh menghubungkan peranti dalam rangkaian global/Internet.
10.	Rangkaian Kawasan Setempat (LAN)	Rangkaian komputer yang menghubungkan peranti dalam satu (1) kawasan terhad (seperti satu (1) bangunan atau pejabat) supaya perkongsian sumber dan komunikasi pengkomputeran dapat dilakukan dengan berkesan.

BAB 1: PENGENALAN

1.1 Tujuan

1.1.1 Garis panduan ini dibangunkan untuk menyokong dan membantu agensi Sektor Awam dalam membuat perancangan keperluan infrastruktur ICT mengikut kaedah yang ditetapkan bagi memastikan agar setiap fasiliti kerajaan dilengkapi dengan infrastruktur ICT yang seragam berdasarkan keperluan teknologi dan inovasi semasa.

1.1.2 Garis panduan ini hendaklah digunakan sebagai dokumen rujukan bagi agensi Sektor Awam Malaysia dalam membangun dan mengoperasikan sistem rangkaian ICT Sektor Awam.

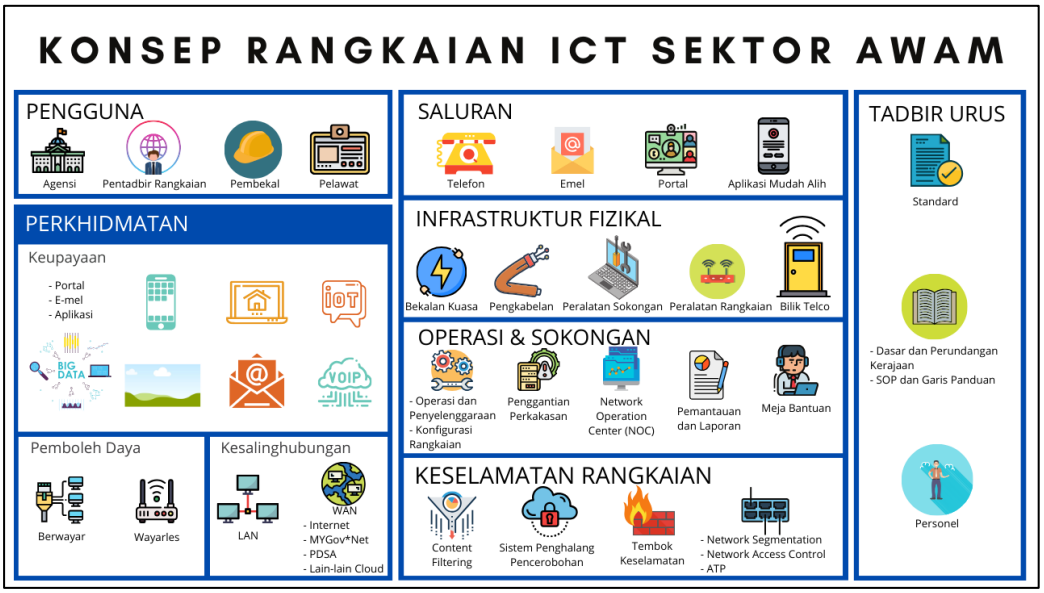
1.2 Pengenalan Rangkaian ICT Sektor Awam

1.2.1 Rangkaian ICT merujuk kepada satu (1) sistem yang menghubungkan pelbagai peranti seperti komputer, pelayan, pencetak, dan peranti lain bagi membolehkan pertukaran data dan perkongsian sumber. Melalui sambungan rangkaian, agensi Sektor Awam dapat menjalankan komunikasi yang lebih pantas, mengurus data secara berpusat, serta meningkatkan kecekapan penyampaian digital agensi Sektor Awam. Rangkaian boleh dibina dalam pelbagai skala, sama ada kecil seperti *Local Area Network* (LAN) dalam sebuah pejabat, mahupun besar seperti *Wide Area Network* (WAN) yang menghubungkan beberapa lokasi geografi. Dalam era digital masa kini, keupayaan rangkaian ICT menjadi tulang belakang kepada sistem maklumat dan operasi teknologi agensi Sektor Awam.

1.2.2 Selain itu, rangkaian ICT memainkan peranan strategik dalam menyokong aspirasi transformasi digital sejajar dengan visi agensi Sektor Awam ke arah perkhidmatan yang lebih cekap, inklusif dan berdaya saing. Infrastruktur rangkaian yang kukuh dan selamat menjadi asas kepada pelaksanaan sistem maklumat bersepadu, pendigitalan perkhidmatan, serta amalan kerja yang berteraskan teknologi. Selaras dengan Pelan Strategik Pendigitalan Sektor Awam (PSPSA) dan Pelan Strategik Pendigitalan (PSP) Agensi, perancangan

dan pembangunan rangkaian ICT perlu dilaksanakan secara menyeluruh, mampan dan berfokus kepada keperluan semasa dan masa depan. Keupayaan rangkaian yang dibina bukan sahaja menyokong kelancaran operasi harian, malah menjadi pemangkin kepada inovasi digital dan pemerkasaan perkhidmatan dalam era ekonomi digital.

1.2.3 Rajah 1.1 menggambarkan konsep rangkaian ICT Agensi Sektor Awam.



Rajah 1.1 Gambar Rajah Konsep Rangkaian ICT Sektor Awam

1.2.4 Ketersediaan ini hanya boleh dicapai dengan memastikan rangkaian dan semua aset ICT kerajaan dilindungi. Selain itu, pemantauan secara berterusan juga perlu bagi memastikan perkhidmatan dan tadbir urus rangkaian yang baik dan optimum.

1.3 Skop Kesediaan Infrastruktur ICT

1.3.1 Garis panduan ini hanya meliputi penyediaan LAN di agensi berdasarkan 4 kategori rangkaian seperti di **Para 3.4.2**. Ia tidak meliputi rangkaian pusat data, WAN seperti satelit dan rangkaian selular.

1.3.2 Bagi memastikan setiap peralatan dan perkhidmatan rangkaian yang dibekalkan di setiap bangunan kerajaan mengikut spesifikasi atau piawaian antarabangsa,

agensi boleh merujuk kepada cadangan tetapan ***Telecommunications Industry Association*** **(TIA), TIA-568, TIA-606, TIA-942, TIA-1152, TIA-1179** dan dokumen **Spesifikasi bagi Peralatan Rangkaian ICT (L-S38** Cawangan Kejuruteraan Elektrik, Jabatan Kerja Raya Malaysia**)** versi terkini.

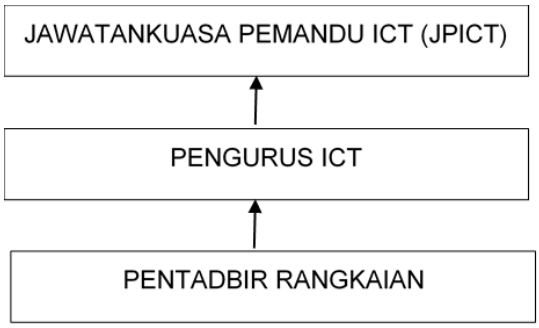
1.3.3 Panduan ini memfokuskan kepada penggunaan teknologi rangkaian semasa dokumen ini dibangunkan. Walau bagaimanapun, agensi juga boleh mengeksplorasi teknologi rangkaian berasaskan *Software Defined Network* (SDN) atau teknologi rangkaian terkini sebagai pilihan dengan melakukan ujian *Proof of Concept* (PoC) atau *Proof of Value* (PoV).

BAB 2: TADBIR URUS

2.1 Tadbir Urus Pembangunan dan Pengoperasian LAN Sektor Awam

2.1.1 Struktur tadbir urus yang kukuh dalam pembangunan dan pengoperasian LAN Sektor Awam adalah penting untuk memastikan keselamatan, kecekapan, dan kebolehpercayaan sistem ICT kerajaan. Struktur ini membantu menetapkan peranan dan tanggungjawab yang jelas, memudahkan pemantauan serta kawalan terhadap penggunaan rangkaian, dan memastikan pematuhan kepada dasar serta piawaian keselamatan siber nasional.

2.1.2 Struktur tadbir urus bagi pembangunan dan pengoperasian LAN di agensi Sektor Awam adalah seperti di Rajah 2.1:



Rajah 2.1: Struktur Tadbir Urus Pembangunan dan Pengoperasian LAN di Agensi

BAB 3: PEMBANGUNAN LAN SEKTOR AWAM

3.1 Pengenalan

3.1.1 LAN merupakan tunjang bagi menyokong perkhidmatan digital kerajaan yang disediakan dengan mematuhi standard dan polisi ICT semasa bagi memastikan ia mudah diurus. Perancangan dan penyediaan perkhidmatan rangkaian juga perlu mengambil kira semua aspek berkaitan perancangan bangunan dengan merujuk kepada **Garis Panduan dan Peraturan bagi Perancangan Bangunan,** Kementerian Ekonomi iaitu:

a. Keperluan ruang untuk menempatkan peralatan di Pusat Data/ Bilik Pelayan*, Telecommunication Closet Room* (TCR), *Riser*, *Subscriber Distribution Frame* (SDF) *Room*, *Main Distribution Frame* (MDF) *Room* dan *Private Automatic Branch Exchange* (PABX)/*KeyPhone Room* dan lain-lain ruang berkaitan.

b. Infrastruktur Pasif, Infrastruktur Aktif serta Sistem Telefoni.

c. Pembangunan Aplikasi.

3.1.2 Dalam mereka bentuk arkitektur rangkaian setempat, pentadbir perlu mengambil maklum berkenaan teknologi terkini dan revolusi teknologi dalam industri. Keperluan awal rangkaian hanyalah menjurus kepada keperluan berbentuk pelanggan/pelayan untuk akses aplikasi yang dihoskan di pusat data. Namun, berikutan perubahan teknologi ke arah pendigitalan perkhidmatan kerajaan, rangkaian perlu dibina berdasarkan keperluan 3 fungsi berikut:

a. Akses berwayar.

b. Akses wayarles.

c. Perancangan kapasiti untuk Teknologi Memuncul (*Emerging Technology*) seperti Internet Benda/*Internet of Things* (IoT) dan Kecerdasan Buatan (AI).

3.1.3 Selain itu, pembangunan dan pengoperasian rangkaian Sektor Awam hendaklah menyokong kelima-lima domain yang disediakan oleh Organisasi Piawaian Antarabangsa ISO/IEC 7498-4 untuk menjamin kebolehpercayaan, keselamatan dan prestasi rangkaian. 5 domain tersebut ialah *Fault Management, Configuration, Accounting, Performance and Security* (FCAPS) seperti berikut:

a. *Fault Management* – keupayaan mengurus segala kerosakan atau gangguan yang berlaku:

   i. mengenal pasti gangguan.
   ii. pengasingan dan diagnosis punca.
   iii. mengatasi gangguan rangkaian.
   iv. analisis serta pemantauan berterusan insiden supaya tidak berulang di masa akan datang.

b. *Configuration* – keupayaan membuat tetapan konfigurasi rangkaian yang betul.

   i. mengurus konfigurasi rangkaian, termasuk tetapan perkakasan, perisian dan sistem pengurusan rangkaian.
   ii. memastikan ketepatan dengan melakukan semakan konfigurasi.
   iii. membuat salinan sandaran konfigurasi untuk pemulihan bencana.
   iv. melaksanakan perubahan pada konfigurasi dengan cara terkawal.

c. *Accounting* – rekod dan dokumentasi rangkaian.

   i. maklumat reka bentuk, topologi, tetapan dan aset yang terlibat dalam rangkaian.
   ii. merekod data penggunaan lebar jalur rangkaian.
   iii. analisis data penggunaan untuk mengenal pasti arah aliran (trend) dan corak.
   iv. laporan untuk perancangan kapasiti dan anggaran peruntukan kos.

d. *Performance* – pengurusan prestasi rangkaian.

i. memantau metrik prestasi rangkaian seperti *bandwidth utilization, throughput, latency, jitter* dan *packet loss.*
ii. mengenal pasti kesesakan prestasi dan mengoptimumkan sumber rangkaian.
iii. melaksanakan penilaian prestasi dan penalaan untuk meningkatkan kecekapan rangkaian selepas penilaian dan penalaan keselamatan rangkaian dilakukan.

e. *Security* – keupayaan mengurus keselamatan rangkaian untuk mengurangkan risiko ancaman keselamatan.

i. pelaksanaan dasar dan prosedur keselamatan ICT untuk melindungi rangkaian daripada ancaman.
ii. pemantauan trafik pelanggaran polisi capaian rangkaian.
iii. tindakan segera terhadap insiden keselamatan rangkaian.
iv. melaksanakan langkah kawalan keselamatan seperti pelaksanaan tembok api, sistem pengesanan pencerobohan dan kawalan akses.

3.1.4 Pendekatan secara reka bentuk atas bawah (*top down design*) adalah dicadangkan supaya selari dengan PSP atau keperluan agensi.

3.2 Kitar Hayat Pembangunan Rangkaian

3.2.1 Terdapat pelbagai model kitar hayat pembangunan rangkaian yang diperkenalkan. Kitar Hayat Pembangunan Rangkaian (*Network Development Life Cycle*, NDLC) merupakan salah satu (1) metodologi pembangunan rangkaian terdiri daripada 5 fasa iaitu analisis, reka bentuk, simulasi, implementasi serta pemantauan dan operasi seperti di Rajah 3.1.

Rajah 3.1 Fasa dalam *Network Development Life Cycle* (NDLC)

3.3 Fasa Analisis

3.3.1 Fasa ini merupakan langkah yang kritikal dalam pembangunan rangkaian ICT. Pada fasa ini, objektif utama adalah untuk menilai keperluan pengguna dan pemegang taruh serta merancang infrastruktur yang sesuai dengan matlamat jangka panjang agensi. Aktiviti utama dalam fasa ini termasuklah analisis keperluan pengguna, penentuan sumber yang diperlukan, serta penilaian risiko yang mungkin timbul semasa pembangunan. Selain itu, perancangan bajet dan pemilihan teknologi yang tepat juga dilakukan untuk memastikan rangkaian yang dibangunkan mampu memenuhi keperluan semasa dan masa depan agensi. Senarai semak keperluan minimum pembangunan dan pengoperasian LAN Sektor Awam adalah seperti di **Lampiran A1**.

3.3.2 **Metodologi pengumpulan maklumat** bagi fasa ini boleh dilakukan dengan kaedah:

a. ***Request For Information* (RFI)** dengan pihak penyedia perkhidmatan bagi memperincikan keperluan rangkaian agensi.

b. **Semakan dokumentasi *blueprintlas-built drawings* dan lawatan tapak** bagi mendapatkan gambaran sebenar keperluan di lokasi termasuk penyediaan pelan bangunan dan gambar rajah elektrikal bangunan, pelan lantai dan sebagainya.

c. **Semakan manual perkakasan** juga diperlukan bagi tujuan mendapatkan maklumat perincian.

d. **Semakan skop dan keperluan** agihan peralatan ICT agensi termasuk jumlah pengguna, aplikasi yang sedang atau akan dibangunkan dan anggaran keperluan akan datang.

e. **Semakan maklumat rangkaian ICT** semasa seperti konfigurasi rangkaian, kapasiti dan penggunaan lebar jalur rangkaian, protokol, kaedah pemantauan rangkaian sedia ada, *Service Level Agreement* (SLA), aduan berkaitan rangkaian melalui meja bantuan dan perancangan keperluan kapasiti akan datang.

f. **Semakan pengurusan fizikal, elektrikal dan penyenggaraan bangunan** seperti keperluan bekalan elektrik, pengkabelan, lokasi, ruang, sistem keselamatan dan perancangan kapasiti fizikal.

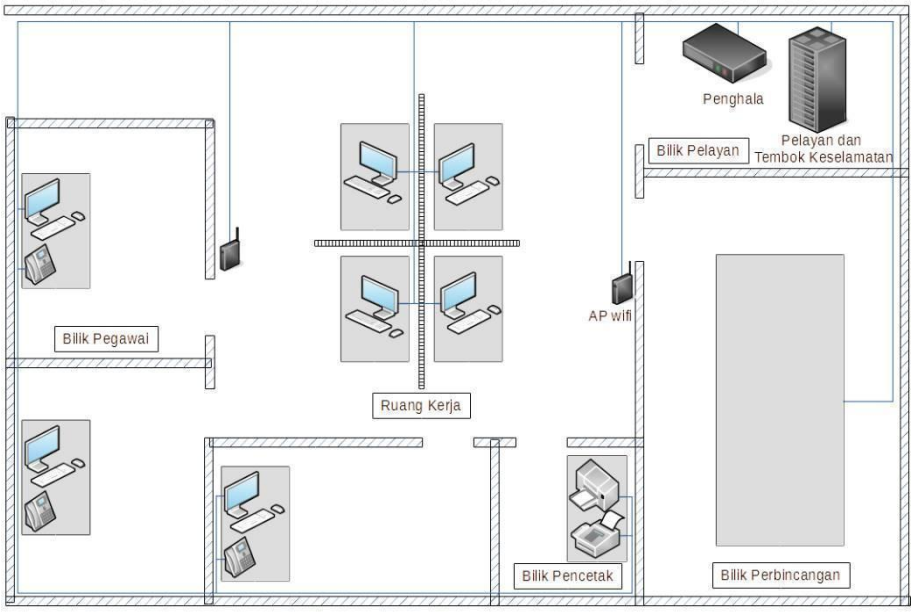
g. **Semakan keperluan dan hala tuju strategik agensi** untuk analisis jurang.

3.4 Fasa Reka Bentuk

3.4.1 Fasa ini bertujuan untuk **menyediakan topologi reka bentuk rangkaian ICT** yang lengkap berhubungan secara fizikal dan logikal. Rajah 3.2 dapat membantu pentadbir merancang susun atur rangkaian struktur topologi, reka bentuk akses data, pengkabelan dan memberi gambaran keperluan awalan yang jelas bagi:

a. **Mereka bentuk topologi rangkaian** berdasarkan reka bentuk hierarki (*Core Layer, Distribution Layer, Access Layer*) bagi keperluan seperti lokasi bilik pelayan, bilik telekomunikasi, lokasi pengguna, lokasi ruang kerja.

b. **Gambar rajah terperinci anggaran keperluan** meliputi carta pelaksanaan, anggaran belanjawan, *work breakout* dan sebagainya.



Rajah 3.2: Contoh Lakaran Susun Atur Komponen Rangkaian

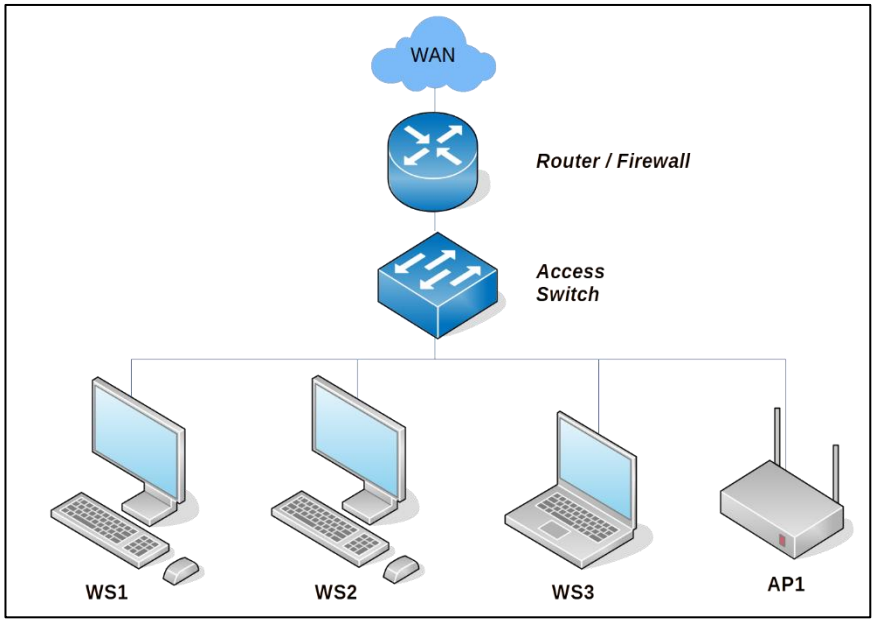
3.4.2 Persekitaran kerja secara digital mengakibatkan keperluan untuk mengakses maklumat tersedia dari mana-mana tanpa mengira waktu. Keperluan tersebut memerlukan rangkaian dengan prestasi yang stabil, selamat dan mempunyai tahap ketersediaan yang tinggi. Pentadbir perlu menyediakan norma keperluan rangkaian berdasarkan 4 kategori berikut:

a. Rangkaian Kategori Kecil

Agensi Sektor Awam yang mempunyai sambungan rangkaian kawasan setempat bersaiz kecil (Rujuk Rajah 3.3) dengan sekurang-kurangnya 1 hingga 24 *port* rangkaian.

Rangkaian kategori ini mengguna pakai konsep asas LAN yang melibatkan unit asas peralatan rangkaian seperti penghala (*router*) dan suis (*switch*) berdasarkan jumlah pengguna seperti dalam gambar rajah di bawah. Tetapan *Dynamic Host Configuration Protocol* (DHCP) dan *Domain Name System* (DNS) boleh dibuat pada penghala atau suis rangkaian.

Fungsi kawalan akses seperti nama pengguna/kata laluan untuk sambungan pengguna terutamanya melalui rangkaian wayarles perlu ada bagi memastikan persekitaran rangkaian yang selamat.



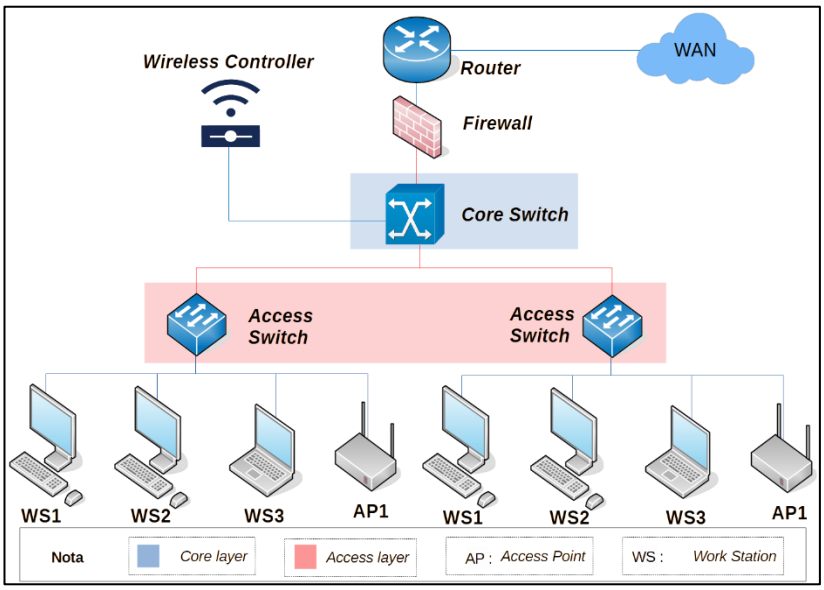
Rajah 3.3: Rangkaian Kategori Kecil

b. Rangkaian Kategori Sederhana

Agensi Sektor Awam yang mempunyai sambungan rangkaian kawasan setempat bersaiz sederhana dengan sekurang-kurangnya 25 hingga 100 *port* rangkaian.

Umumnya reka bentuk Rangkaian Kategori Sederhana adalah berdasarkan saiz, ruang dan jumlah aras di dalam bangunan. Terdapat keperluan untuk menyediakan satu (1) ruang atau bilik komputer bagi menempatkan peralatan rangkaian khusus bagi memudahkan penyelenggaraan. Tetapan DHCP dan DNS boleh dibuat pada penghala atau suis rangkaian atau pelayan berasingan. Fungsi kawalan akses seperti nama pengguna/kata laluan untuk sambungan pengguna melalui rangkaian wayarles perlu ada bagi memastikan persekitaran rangkaian yang selamat. Integrasi bersama Pelayan Direktori *(Directory Server*) sangat digalakkan untuk kawalan akses pengguna ke persekitaran rangkaian. Reka bentuk pengasingan boleh diperkenalkan bagi

mengasingkan trafik dan segmen pengguna yang bertujuan untuk meningkatkan tahap keselamatan seperti di Rajah 3.4.



Rajah 3.4: Rangkaian Kategori Sederhana

c. Rangkaian Kategori Besar

Agensi Sektor Awam yang mempunyai sambungan rangkaian setempat bersaiz besar (Rujuk Rajah 3.5) yang melebihi 100 *port* rangkaian.

Agensi yang mempunyai beberapa buah bangunan di dalam kawasan yang sama boleh dikategorikan sebagai rangkaian sederhana besar multi lokasi atau Rangkaian Kategori Besar. Bagi memenuhi keperluan rangkaian kategori ini, perkara asas seperti berikut dijadikan panduan:

i. **Hierarki**: Reka bentuk hierarki (*access layer, distribution layer, core layer*) membolehkan setiap peralatan pada setiap peringkat dapat difahami dengan jelas tentang peranan dan fungsi masing-masing bagi memudahkan pelaksanaan, operasi, pengurusan dan mengurangkan kegagalan pada setiap peringkat tersebut.

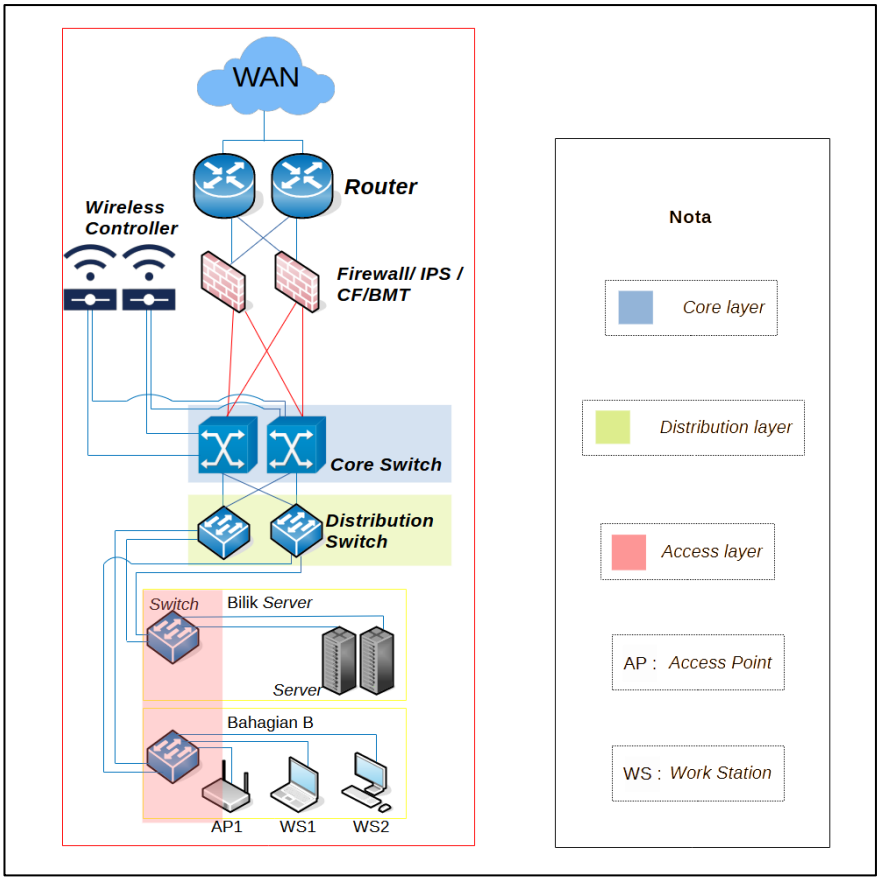
ii. **Prestasi Stabil**: Lebar jalur (*bandwidth*) yang diperlukan dan dibekalkan mencukupi serta boleh dikawal. Jumlah lebar jalur boleh ditetapkan berdasarkan jumlah lebar jalur yang akan disediakan untuk setiap pengguna. Pemantauan prestasi rangkaian melibatkan komponen seperti *bandwidth utilization, latency* dan *packet loss*. Kawalan sekatan capaian ke laman tidak produktif yang boleh menyesakkan dan mengganggu kestabilan prestasi rangkaian. Perkakasan dengan fungsi *Uniform Resource Locator* (URL)/*Content Filtering* (CF) atau *Bandwidth Management Tool* (BMT) boleh dipertimbangkan untuk pelaksanaan.

iii. **Selamat**: Fungsi kawalan capaian ke perkakasan rangkaian sama ada berwayar ataupun wayarles perlu ada. Perkakasan dengan fungsi tembok keselamatan (*Next Generation Firewall*, NGFW), tetapan *Network Time Protocol* (NTP) selari pada semua perkakasan rangkaian dan integrasi Pelayan Direktori/*Identity Access Management* (IAM) *Server* boleh dilaksanakan. Pastikan log disimpan sekurang-kurangnya 6 bulan bagi tujuan jejak audit.

iv. **Ketahanan (*Resilience*)**: Fungsi *redundancy* juga perlu ada pada perkakasan rangkaian bagi memastikan tahap ketersediaan dan ketahanan yang tinggi.

v. **Boleh Skala (*Scalable*)**: Membolehkan rangkaian diperluaskan atau diintegrasi dengan perkhidmatan ataupun perkakasan lain dengan mudah melalui penetapan konfigurasi berdasarkan protokol piawaian terbuka (*open standard protocol*) sekiranya terdapat keperluan untuk menampung pertambahan pengguna pada masa akan datang.

Sambungan fizikal beberapa buah bangunan disambungkan dengan gentian optik (*fiber optic*) *multimode* atau *single mode* mengikut jarak yang bersesuaian.



Rajah 3.5: Rangkaian Kategori Besar

d. Rangkaian Kategori Kampus

Merupakan sambungan rangkaian kawasan setempat berskala besar (Rujuk Rajah 3.6 dan Rajah 3.7) yang meliputi beberapa agensi Sektor Awam. Kategori rangkaian ini juga dikenali sebagai rangkaian kampus. Contoh rangkaian kampus adalah *Putrajaya Campus Network* (PCN) dan rangkaian komputer universiti awam Malaysia.

Rangkaian ini mengadaptasi reka bentuk multi bangunan dengan setiap lapisan untuk menyokong fungsi dan servis seperti menyediakan arkitektur dengan prestasi yang stabil, tahap ketersediaan yang tinggi, tahap keselamatan yang tinggi, boleh skala, mempunyai ciri *visibility*, analitik dan kesediaan untuk diintegrasi dengan pembekal atau rangkaian lain. Penggunaan reka bentuk *tier* untuk rangkaian yang berskala besar mempunyai kelebihan seperti mudah diurus dan fleksibel bagi tujuan

penyelenggaraan dan menampung pertambahan peralatan atau perkhidmatan.

Selain daripada panduan untuk rangkaian kategori besar yang telah dinyatakan sebelum ini, reka bentuk rangkaian multi lokasi juga boleh mengambil kira beberapa faktor utama seperti berikut:

i. **Prestasi**: Lebar jalur yang diperlukan dan dibekalkan mestilah mencukupi, boleh dikawal dan stabil. Perkakasan rangkaian yang akan digunakan mestilah boleh menampung lebar jalur trafik yang lebih besar. Reka bentuk berprestasi tinggi seperti *core switch* yang menyokong minimum 10 Gigabit Ethernet, *non-blocking switches*, fungsi *link aggregation* dan fungsi *Quality of Services* (QoS) boleh digunakan.

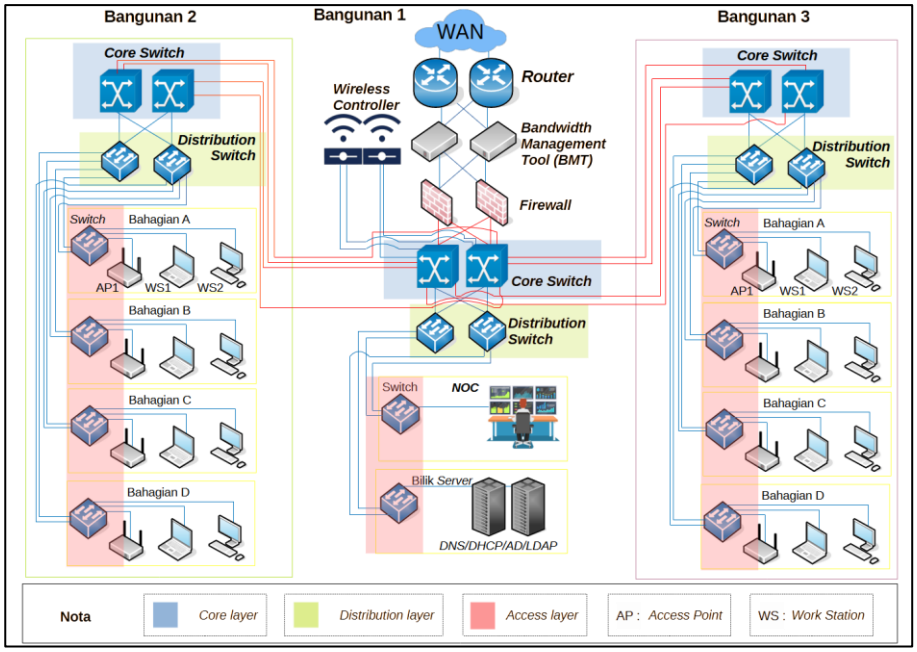
ii. **Selamat**: Kawalan pengasingan pelbagai segmen rangkaian secara mikro dan makro melalui *Virtual Local Area Network* (VLAN)/ *Dynamic Segmentation* (*Dynamic* VLAN) mengikut fungsi pengguna atau *Physical Port Segmentation*. Kawalan Akses Rangkaian (*Network Access Control* atau NAC), *Port Security* dan *Access Control Lists* (ACL)/NGFW boleh digunakan agar pengguna yang dibenarkan sahaja dapat mengakses rangkaian tersebut.

iii. **Ketahanan (*Resilience*)**: Ketersediaan dengan ketahanan selaras Tahap Jaminan Perkhidmatan (SLG) lebih tinggi. Pelaksanaan secara *redundancy* untuk suis rangkaian, tembok keselamatan, pengawal wayarles LAN (WLC), CF, *Advanced Threat Protection* (ATP), *power supply module* dan talian rangkaian (*horizontal, vertical & inter-building*).

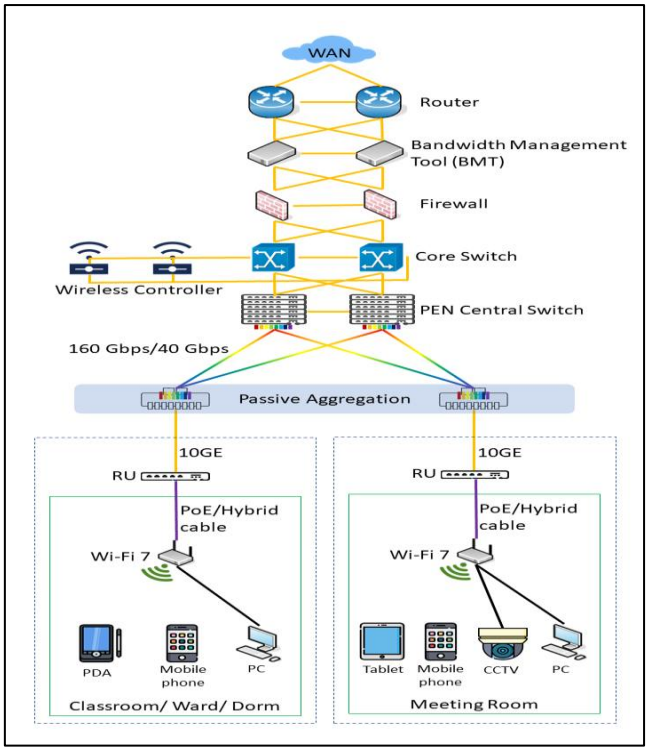
iv. **Saling kendali (*Interoperability*)**: Menyokong sepenuhnya piawaian IEEE atau piawaian terbuka yang dapat memastikan saling boleh kendali antara peralatan rangkaian daripada pelbagai pembekal.

v. **Pengurusan**: Mempunyai sistem pengurusan dan pemantauan yang menyokong pengurusan perkakasan dan perisian rangkaian untuk digunakan oleh pentadbir rangkaian pelbagai agensi. Penggunaan *network orchestrator*, WLC dengan fungsi telemetri dan analitik boleh dipertimbangkan untuk pelaksanaan.

vi. **Boleh Skala (*Scalable*)**: Suis LAN pada lapisan *distribution* atau *core* dengan dilengkapi dengan ciri modular, *multilayer*, *high-speed* bagi membolehkan peluasan rangkaian yang memenuhi keperluan sambungan rangkaian ke bangunan baharu dan pengguna pada masa akan datang. *Backplane* berkapasiti tinggi contohnya Terabit sesaat berkeupayaan untuk menyokong keperluan sambungan 40/100 *Gigabit Ethernet* ataupun lebih tinggi pada masa akan datang.



Rajah 3.6: Rangkaian Kategori Kampus



Rajah 3.7: Rangkaian Kategori Kampus (alternatif)

3.5 Fasa Simulasi

3.5.1 **Fasa Simulasi** boleh dilaksanakan bagi menggambarkan pengoperasian rangkaian ICT yang sebenar. Terdapat pelbagai aplikasi simulasi rangkaian yang boleh digunakan untuk melaksanakan simulasi model rangkaian yang telah disediakan semasa Fasa Reka Bentuk seperti *Graphical Network Simulator*, *Packet Tracer, NetSim* dan sebagainya.

3.5.2 Agensi digalakkan untuk **melaksanakan PoC/PoV bagi menilai peralatan rangkaian** yang terdapat di pasaran tanpa melibatkan sebarang kos atau obligasi kepada kerajaan. Agensi boleh melaksanakan simulasi atau pengujian di makmal yang disediakan oleh pihak pembekal peralatan.

3.5.3 Sekiranya Agensi memilih untuk **melaksanakan simulasi di bangunan sendiri**, Agensi hendaklah meminimumkan *downtime* khususnya yang melibatkan aplikasi kritikal kerajaan. Ini boleh dicapai melalui pelaksanaan simulasi di luar waktu pejabat.

3.6 Fasa Implementasi

3.6.1 **Fasa Implementasi** merupakan tahap penting pembangunan rangkaian yang telah dirancang. Rujukan dokumen Spesifikasi untuk Sistem Rangkaian ICT L-S38 yang dibangunkan bersama pasukan Cawangan Kejuruteraan Elektrik JKR boleh dirujuk sebagai panduan pelaksanaan. Spesifikasi kabel *Unshielded Twisted Pair* (UTP) Cat 6A, kabel gentian optik *multimode* 4/5 (OM4/OM5) dan kabel gentian optik *singlemode* 2 (OS2) juga ditetapkan sebagai pilihan untuk digunakan dalam pembangunan rangkaian.

3.6.2 Bagi memastikan rangkaian berfungsi seperti yang dirancang, beberapa pengujian perlu dilaksanakan termasuk *User Acceptance Test* (UAT), *Provisional Acceptance Test* (PAT) dan *Final Acceptance Test* (FAT):

a. *User Acceptance Test* (UAT)

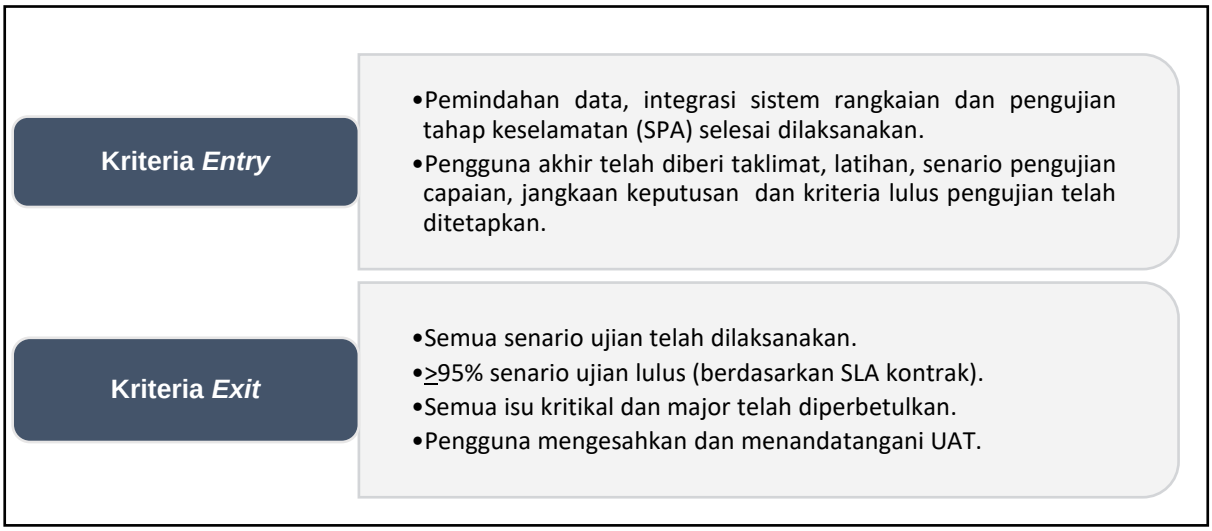
i. UAT melibatkan pengguna akhir (*end user*) untuk memastikan pembangunan rangkaian memenuhi keperluan pengoperasian dan fungsi yang ditetapkan.

ii. Memberi tumpuan terhadap fungsi perkhidmatan rangkaian, kemudahan penggunaan, proses dan simulasi capaian seperti senario sebenar yang dipersetujui pengguna akhir.

iii. Langkah-langkah pelaksanaan UAT:

- Pemindahan data, integrasi sistem rangkaian dan pengujian tahap keselamatan (SPA) selesai dilaksanakan.
- Pengujian ini melibatkan penilaian prestasi capaian rangkaian.
- Mendokumenkan hasil pengujian dan sebarang isu yang dikenal pasti akan diselesaikan sebelum pelaksanaan PAT.

iv. Kriteria *Entry* dan Kriteria *Exit* bagi UAT adalah di Rajah 3.8.



Rajah 3.8: Kriteria *Entry* dan Kriteria *Exit* bagi UAT

b. *Provisional Acceptance Test* (PAT)

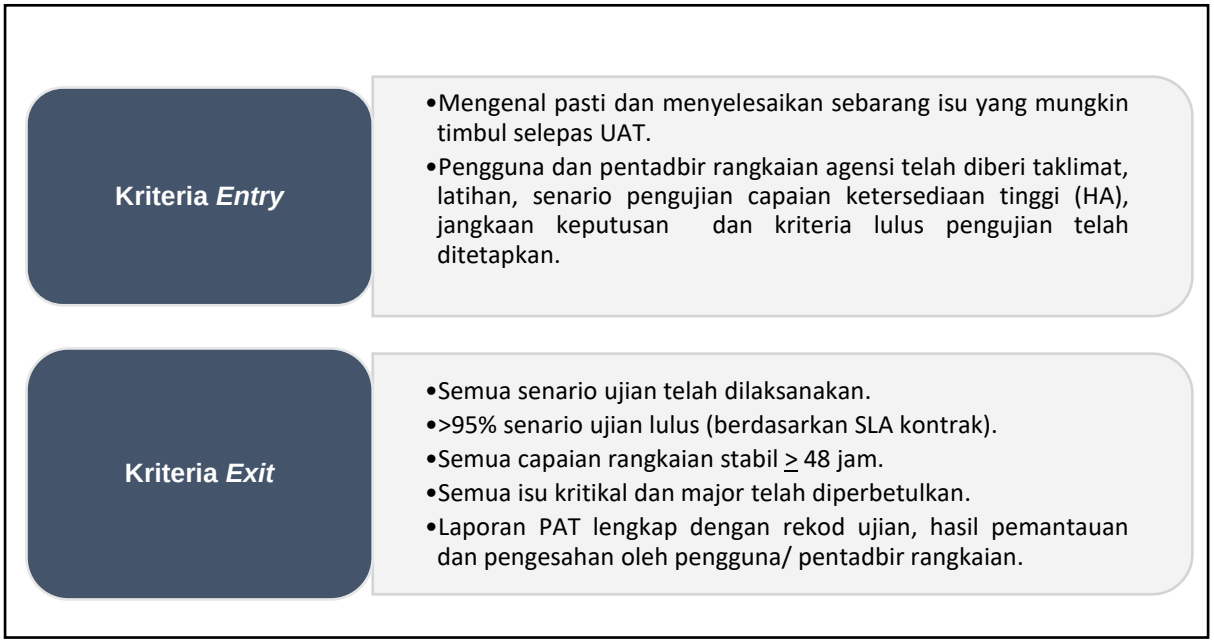
i. Pengujian selepas UAT yang bertujuan untuk memastikan sistem rangkaian dapat beroperasi secara stabil dalam persekitaran sebenar sebelum dapat digunakan sepenuhnya.

ii. Memberi tumpuan terhadap fungsi perkhidmatan rangkaian, kemudahan penggunaan, proses dan simulasi capaian seperti senario sebenar (termasuk senario kegagalan), ketersediaan tinggi (HA) dan capaian dari pelbagai bangunan yang dipersetujui melibatkan pelbagai pengguna/pentadbir rangkaian.

iii. Langkah-langkah pelaksanaan PAT:

- Pastikan persekitaran perkakasan dan perisian rangkaian dari pelbagai pengguna/bangunan melalui rangkaian ketersediaan tinggi (HA) boleh diuji.
- Pengujian ini melibatkan penilaian prestasi capaian rangkaian.
- Mendokumentasi perkara yang perlu ditambah baik sebelum pengujian seterusnya iaitu *Final Acceptance Test* (FAT) dilaksanakan.

v. Kriteria *Entry* dan Kriteria *Exit* bagi PAT adalah di Rajah 3.9.



Rajah 3.9: Kriteria *Entry* dan Kriteria *Exit* bagi PAT

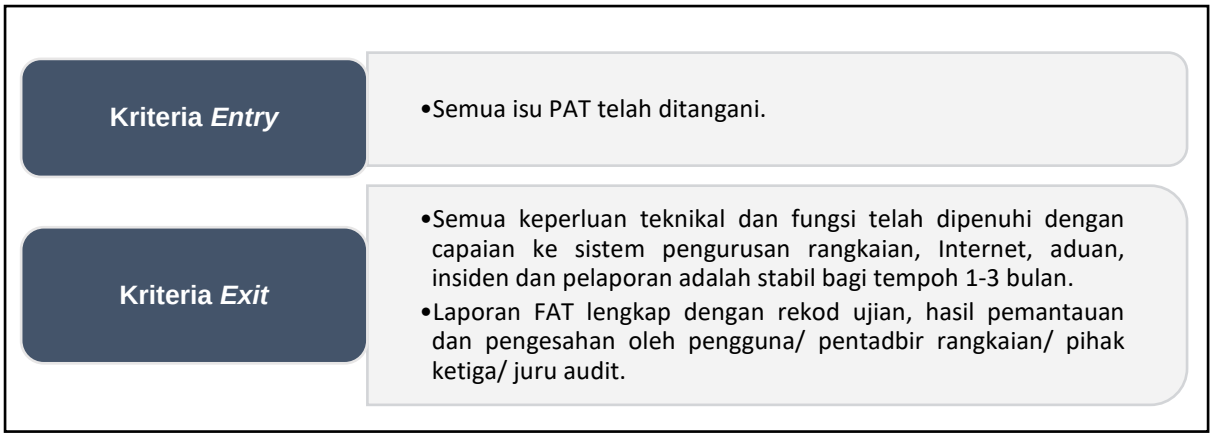
c. *Final Acceptance Test* (FAT)

i. FAT ialah pengujian akhir yang dilaksanakan bersama pengguna/ pentadbir rangkaian/ pihak ketiga/ juru audit untuk memastikan rangkaian memenuhi semua keperluan teknikal dan operasi dengan stabil seperti yang dinyatakan dalam spesifikasi dan kontrak projek.

ii. Langkah-langkah pelaksanaan FAT:

- Dilaksanakan selepas UAT/ PAT selesai dan pengguna membuat pengesahan prestasi rangkaian.
- Menguji kestabilan keseluruhan fungsi termasuk integrasi antara komponen, pemantauan, pengurusan, pelaporan dan penyelesaian semua insiden rangkaian.
- Memastikan tiada isu kritikal yang tertinggal.
- Mendokumenkan hasil pengujian dan laporan akhir secara rasmi.

iii. Kriteria *Entry* dan Kriteria *Exit* bagi FAT adalah di Rajah 3.10.



Rajah 3.10: Kriteria *Entry* dan Kriteria *Exit* bagi FAT

3.6.3 Dengan melaksanakan UAT, PAT dan FAT agensi dapat memastikan bahawa rangkaian LAN yang dibangunkan memenuhi keperluan pengguna, berfungsi dengan baik dan sedia untuk beroperasi dengan risiko yang minimum. Contoh templat **Senarai Semak Pengujian Rangkaian** boleh dirujuk di **Lampiran A2**.

3.6.4 Walau bagaimanapun, terdapat beberapa cabaran dari aspek teknikal dan bukan teknikal yang memerlukan pengurusan projek dan pengurusan risiko bagi tujuan meminimumkan risiko kegagalan projek di antaranya seperti berikut:

a. Jadual pelaksanaan yang tidak tepat kerana perancangan atau pemahaman fungsi yang tidak tepat disebabkan oleh kekangan pada perkakasan/sistem.
b. Kekurangan peruntukan, perubahan polisi organisasi atau perubahan reka bentuk.
c. Semangat berpasukan yang tidak jitu atau tiada rasa kepunyaan (*sense of belonging*).
d. Isu peralatan sokongan.
e. Pembekal kurang pengalaman.

Pasukan projek disarankan untuk melaksanakan projek ICT berdasarkan **Panduan Pengurusan Projek ICT Sektor Awam (PPrISA)**.

3.7 Fasa Pemantauan dan Operasi

3.7.1 **Fasa pemantauan dan operasi** melibatkan aktiviti pemantauan dan pengurusan.

3.7.2 **Aktiviti Pemantauan -** Khusus untuk menjamin agar rangkaian ICT dapat beroperasi secara optimum berdasarkan keperluan pengguna melalui analisis secara terperinci. Kebolehpercayaan perkakasan rangkaian hendaklah dipantau sekurang-kurangnya dari aspek ketersediaan, keselamatan dan prestasi.

3.7.3 Agensi perlu melaksanakan pemantauan rangkaian berterusan bagi memastikan SLA/*Key Performance Indicator* (KPI) rangkaian sentiasa tercapai. Penggunaan aplikasi Sistem Pemantauan Rangkaian (*Network Management System*, NMS) yang mempunyai ciri AI dan pemantauan secara berpusat adalah digalakkan bagi memastikan kawalan dan pemantauan yang menyeluruh di semua peringkat.

3.7.4 **Aktiviti Pengurusan -** Asas aktiviti pengurusan adalah berdasarkan kerangka FCAPS untuk memastikan semua aspek rangkaian, termasuk prestasi, keselamatan, kestabilan, dan pematuhan polisi, diuruskan dengan cekap. Polisi penggunaan rangkaian perlu ditambah baik dan diselaraskan dengan mengambil kira Dasar Keselamatan ICT (DKICT)/Polisi Keselamatan Siber (PKS) agensi bagi memastikan rangkaian yang dibangunkan beroperasi dengan baik, selamat, berdaya tahan dan berprestasi pada tahap yang optimum.

BAB 4: PERALATAN/ KOMPONEN RANGKAIAN

4.1 Pengenalan

4.1.1 Senarai perkhidmatan dan peralatan yang diperlukan bagi mengoperasikan LAN adalah termasuk segala peralatan rangkaian serta sistem perisian dan operasi rangkaian.

4.2 Peralatan dan Perkhidmatan Rangkaian

4.2.1 Secara umumnya infrastruktur rangkaian mengandungi 3 kategori komponen rangkaian utama iaitu peralatan rangkaian, media rangkaian (*cabling*) dan perisian (*software and services*). Berikut adalah senarai perkhidmatan rangkaian yang diperlukan bagi setiap agensi:

a. Alamat IP (IP *Address*)

i. Alamat IP ialah nombor pengalamatan IPv4 dan IPv6 unik yang diberikan kepada komputer, pencetak, suis, penghala dan peralatan rangkaian lain bagi membolehkan ia disambung kepada rangkaian dalaman atau Internet. **Terdapat 3 kaedah penyediaan alamat IP bagi agensi Sektor Awam iaitu**:

- **Agensi di bawah MyGov*Net** akan dibekalkan sejumlah alamat IP dalaman dan luaran dengan konfigurasi dilaksanakan sendiri oleh agensi.
- **Agensi melanggan Pembekal Khidmat Internet** (*Internet Service Provider* atau ISP) selain MyGov*Net akan diperuntukkan alamat IP dalaman dan luaran yang disediakan oleh Penyedia Perkhidmatan Internet.
- **Agensi yang tiada perkhidmatan Rangkaian Kawasan Luas** (WAN) perlu menguruskan alamat IP secara sendiri.

ii. Agensi hendaklah merancang dan memastikan kesediaan untuk beralih kepada penggunaan alamat IPv6 sepertimana yang telah dinyatakan dalam **Surat Arahan Ketua Pengarah MAMPU Tahun 2010 Garis Panduan Transisi IPv6 Sektor Awam** atau mana-mana arahan/panduan terkini.

Pelan migrasi bagi penggunaan alamat IPv6 perlu disediakan dengan menetapkan objektif untuk melaksanakan penggunaan **alamat IPv6 secara natif** di keseluruhan rangkaian agensi, termasuk di semua pejabat cawangan. Sebelum migrasi dilaksanakan, semakan terhadap ketersediaan perkakasan, sistem rangkaian dan aplikasi sedia ada perlu dilakukan. Selain itu, ujian capaian secara horizontal (antara bangunan atau agensi) dan ujian capaian secara vertikal (ke atau dari Internet) perlu dilaksanakan bagi memastikan proses migrasi rangkaian berjalan dengan lancar dan berfungsi seperti yang dirancang.

iii. Agensi hendaklah merujuk kepada **pasukan projek Pusat Data Sektor Awam (PDSA) dan MyGov*Net dalam menetapkan skema IP** bagi memastikan penggunaan alamat IP tidak bertindih, memudahkan integrasi dan migrasi alamat IP.

iv. Agensi tidak digalakkan untuk mengguna pakai kaedah ***Network Address Translation*** **(NAT)** yang boleh meminimumkan prestasi capaian dan kesukaran membuat pemantauan/pengurusan/ *troubleshooting* dalaman LAN.

b. Tembok Keselamatan (*Firewall/Next Generation Firewall*)

i. Tembok keselamatan merupakan sistem keselamatan utama bagi rangkaian di agensi yang berfungsi untuk memantau dan mengawal aliran keluar masuk trafik berdasarkan polisi yang ditetapkan oleh pentadbir rangkaian.

ii. Tembok keselamatan bertujuan untuk memberikan lapisan perlindungan tambahan yang penting dan dilengkapi dengan ciri-ciri seperti *Virtual Private Network* (VPN), kemudahan akses dari luar (*remote access*), *Intrusion Prevention System* (IPS) dan web CF. Pemilihan tembok keselamatan mestilah bersesuaian dengan keperluan agensi.

iii. Tembok keselamatan perlu diletakkan pada lokasi strategik untuk mengawal komunikasi antara zon/segmen luaran, dalaman dan *Demilitarized Zone* (DMZ). Polisi keselamatan perlu dilaksanakan pada setiap segmen tersebut bagi mengawal capaian pengguna dan disemak dari semasa ke semasa untuk memastikan keselamatan rangkaian berada di tahap optimum.

iv. Bagi agensi dengan rangkaian kategori kecil, digalakkan untuk menggunakan tembok keselamatan atau fungsi kawalan keselamatan terbina dalam (*built-in*) yang terdapat pada penghala/suis yang dibekalkan oleh penyedia perkhidmatan.

c. Pengurusan Akses berasaskan *Identity Access Management* (IAM)

i. Penggunaan Perkhidmatan Direktori (*Directory Services*) seperti *Active Directory* (AD) atau *Lightweight Directory Access Protocol* (LDAP) boleh digunakan untuk mengurus pengguna yang mempunyai akses kepada rangkaian dalaman.

ii. Agensi perlu mengemaskini maklumat pengguna terkini dari semasa ke semasa.

iii. Agensi digalakkan untuk mengintegrasi pelayan AD/LDAP dengan perkakasan rangkaian yang mempunyai tetapan polisi capaian pengguna seperti tembok keselamatan dan WLC untuk membolehkan kawalan akses dan pelaporan dibuat berdasarkan pengguna.

d. Pelayan DHCP

Agensi digalakkan untuk menyediakan pelayan DHCP untuk merekod agihan alamat IP secara automatik bagi mengelakkan masalah konflik alamat IP. Digalakkan juga untuk mengasingkan skop tetapan alamat IP bagi pengguna berwayar dan wayarles.

e. Pelayan DNS

Agensi perlu menyediakan DNS untuk pengenalan nama domain, *resolve* dan *queries*. Pelayan DNS terdiri daripada dua jenis kategori iaitu DNS dalaman (*internal* DNS) dan DNS luaran (*external* DNS). Agensi perlu mengenal pasti peranan agensi dalam pengurusan *internal* dan *external* DNS. Agensi pengguna MyGov*Net dikehendaki menggunakan DNS yang disediakan oleh perkhidmatan MyGov*Net.

f. *Virtual Local Area Network* (VLAN)

i. Agensi digalakkan untuk mewujudkan VLAN bagi melaksanakan segmentasi ke atas peralatan rangkaian secara logikal berdasarkan keperluan kumpulan atau fungsi kerja setiap bahagian pengguna bagi tujuan keselamatan akses dan polisi trafik rangkaian tanpa dipengaruhi oleh kedudukan fizikal.

ii. *Gateway* setiap VLAN pengguna boleh diletakkan pada penghala, tembok keselamatan, *core switch* atau mana-mana peralatan mengikut kesesuaian bagi membolehkan kawalan antara VLAN pengguna dilaksanakan.

4.3 Integrasi Rangkaian MyGov*Net

4.3.1 **Rangkaian MyGov*Net dan Putrajaya Campus Network (PCN) -** Agensi yang mengguna pakai talian MyGov*Net atau PCN perlu mematuhi polisi penggunaan semasa yang berkuatkuasa.

4.3.2 Agensi yang tidak mengguna pakai talian MyGov*Net adalah bertanggungjawab sepenuhnya ke atas permohonan talian rangkaian Internet dan WAN melalui penyedia perkhidmatan masing-masing. Agensi perlu mengambil kira kos integrasi dengan rangkaian MyGov*Net sekiranya diperlukan. Setiap titik integrasi mestilah mempunyai kawalan capaian supaya ancaman keselamatan dari rangkaian luar atau pihak ketiga boleh disekat dari memasuki rangkaian MyGov*Net dan rangkaian agensi.

BAB 5: RANGKAIAN WAYARLES

5.1 Pengenalan

5.1.1 Perkembangan ICT membolehkan maklumat dihantar dan diterima dengan pantas. Salah satu (1) teknologi komunikasi yang semakin luas penggunaannya dalam Sektor Awam ialah teknologi rangkaian wayarles. Selain daripada mempercepatkan komunikasi, teknologi ini lebih mudah dan murah untuk dilaksanakan berbanding pelaksanaan rangkaian berwayar. Ia juga mengurangkan kebergantungan terhadap peranti atau perkakasan komputer yang disediakan oleh jabatan dengan menyokong pelaksanaan *Bring Your Own Device* (BYOD) dan memberi kebebasan untuk membuat capaian dari pelbagai lokasi dan akan memudahkan pelaksanaan tugas harian.

5.2 Piawaian Teknologi Rangkaian Wayarles

5.2.1 Piawaian teknologi komunikasi wayarles adalah merujuk kepada penetapan protokol komunikasi wayarles yang dipersetujui di peringkat antarabangsa dan industri untuk digunakan dalam sistem komunikasi antara perkakasan ataupun peranti yang membolehkan pemindahan data tanpa melibatkan sambungan fizikal.

5.2.2 Piawaian berkaitan rangkaian wayarles dibangunkan oleh Institute of Electrical and Electronics Engineers (IEEE). Beberapa contoh piawaian wayarles LAN adalah termasuk (Rujuk Rajah 5.1):

Jadual 5.1: Piawaian Wayarles LAN

Generasi	**Piawaian IEEE**	**Diguna pakai**	***Maximum Linkrate* (Mbit/s)**	***Radio Frequency* (GHz)**
Wi-Fi 8	802.11bn	Dijangka 2028	Dijangka $\geq$ 46120	2.4/5/6
Wi-Fi 7	802.11be	2024	1376 - 46120	2.4/5/6
Wi-Fi 6E	802.11ax	2020	574 - 9608	6
Wi-Fi 6		2019		2.4/5

5.3 Pelaksanaan Rangkaian Wayarles

5.3.1 Terdapat beberapa aktiviti utama yang perlu dilakukan untuk pelaksanaan rangkaian wayarles. Antaranya adalah:

a. Penetapan keperluan keseluruhan, analisis jurang dan perancangan.

b. Tinjauan awal tapak, cadangan tetapan reka bentuk, cadangan tetapan ruang pejabat yang memerlukan wayarles, semakan gangguan signal frekuensi wayarles lain dan teknologi bersesuaian.

c. Semakan liputan signal spektrum frekuensi radio, perancangan kapasiti dan peta haba (*heat map*) dengan kekuatan **signal wayarles minimum: -67dBm (*Received Signal Strength Indicator*, RSSI)**.

d. Tinjauan manual liputan signal spektrum frekuensi radio (AP *on a stick*).

e. Semakan akhir reka bentuk, alamat IPv4 dan IPv6, keselamatan dan pilihan perkakasan.

f. Pemasangan, penetapan konfigurasi, penilaian keselamatan, penilaian prestasi dan penyediaan dokumentasi.

g. Pemantauan berterusan dan pengoptimuman prestasi capaian rangkaian wayarles.

5.3.2 **Penetapan keperluan keseluruhan, analisis jurang dan perancangan**

Dalam fasa ini keperluan utama bisnes agensi, status semasa pelaksanaan rangkaian wayarles dan jurang perbezaan keperluan rangkaian wayarles agensi dikenal pasti. Objektif pelaksanaan rangkaian wayarles ditetapkan. Contohnya, pemasangan rangkaian wayarles adalah untuk mengatasi isu liputan signal yang tidak mencukupi, menaik taraf wayarles AP untuk menyokong pertambahan kapasiti lebar jalur, keperluan sambungan perkakasan IoT atau pemasangan

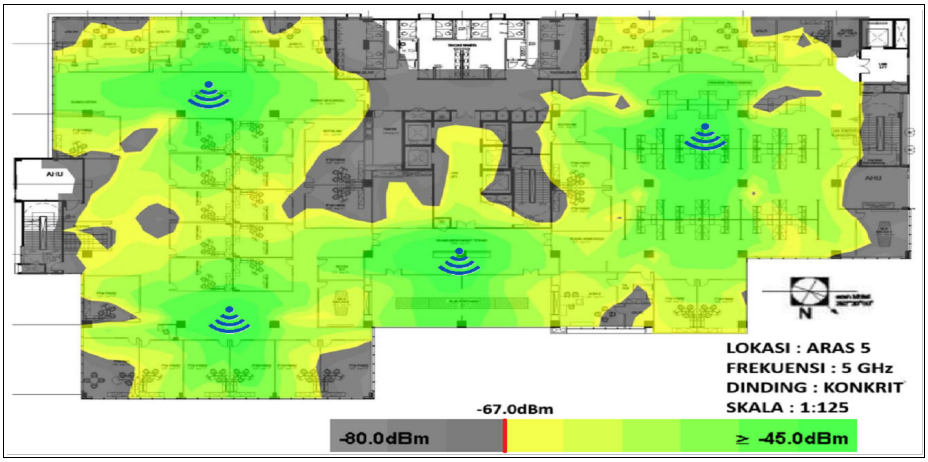
adalah untuk menggantikan perkakasan usang (*End of Sale/Support* atau EOS) yang tidak menyokong keperluan keselamatan terkini. Perancangan awal reka bentuk boleh ditetapkan berdasarkan maklumat kawasan liputan terlibat, jangkaan bilangan aplikasi/perkakasan yang akan disambung dan pengguna rangkaian wayarles. Semakan awal teknologi dan produk wayarles juga dibuat bagi mengenal pasti jenis wayarles AP/WLC yang mungkin akan digunakan.

5.3.3 Tinjauan awal tapak

Semasa tinjauan awal, semakan fizikal seperti ketinggian siling, ketebalan dinding konkrit, dinding kaca, jenis pintu, telefon *bluetooth*, wayarles AP lain, ketuhar gelombang mikro, smart TV/projektor, wayarles CCTV, pengesan (*sensor*) IoT, kepadatan pengguna dan penentuan laluan kabel dibuat. Semakan frekuensi wayarles lain yang boleh mengganggu atau memberi kesan terhadap kawasan liputan signal WLAN juga dilakukan. Perisian perancangan/ tinjauan wayarles yang terdapat di pasaran boleh digunakan untuk pembangunan peta haba (*heat map*).

5.3.4 Semakan liputan signal spektrum frekuensi radio dan perancangan kapasiti

Semakan liputan ini boleh dilaksanakan menggunakan perisian perancangan/ tinjauan peta haba. Maklumat yang diperoleh semasa tinjauan awal tapak bersama pelan lantai boleh digunakan untuk mendapatkan anggaran awal liputan signal, lokasi sesuai pemasangan wayarles AP, jenis wayarles AP dan bilangan wayarles AP. Liputan dengan kekuatan signal RSSI minima **-67dBm** boleh dijadikan panduan sebagai kekuatan signal minimum diperlukan untuk pengguna menggunakan WLAN dengan baik. Rajah 5.1 menunjukkan contoh peta haba bagi rangkaian wayarles.



Rajah 5.1: Contoh Peta Haba bagi Rangkaian Wayarles

5.3.5 Tinjauan fizikal liputan signal spektrum frekuensi radio

Setelah cadangan awal lokasi untuk pemasangan AP dikenal pasti melalui penggunaan perisian, semakan liputan secara fizikal dilakukan. Ini adalah untuk mengenal pasti ketepatan hasil tinjauan melalui perisian sebelum ini. Proses ini boleh dilakukan dengan memasang AP *on a stick*, komputer riba dan telefon bimbit. AP dibawa ke lokasi cadangan pemasangan dan liputan signal disemak berdasarkan kekuatan signal frekuensi radio (RSSI minimum: **-67dBm**) yang diterima di komputer riba dan telefon bimbit. *Signal-to-Noise Ratio* (SNR) yang merupakan parameter kritikal dalam menentukan kualiti sambungan dan kelajuan sebenar capaian seperti Jadual 5.2 boleh digunakan sebagai rujukan. Cadangan lokasi pemasangan AP ditetapkan semasa tinjauan fizikal ini.

Jadual 5.2: Piawaian *Signal-to-Noise Ratio* (SNR) Wayarles LAN

Aplikasi	SNR Minimum Disarankan
Aplikasi biasa (web, emel)	≥ 20 dB
Suara / video masa nyata	≥ 25–30 dB
Pengguna kritikal	≥ 35–40 dB

5.3.6 Semakan akhir reka bentuk

Semakan akhir reka bentuk dibuat selaras dengan teknologi dan produk wayarles yang akan digunakan. Piawaian wayarles, ciri-ciri keselamatan dan fungsi-fungsi wayarles untuk memudahkan proses *onboarding*, pemantauan,

keupayaan integrasi dengan IAM/AD/LDAP, *troubleshooting* dan pelaporan ditetapkan.

5.3.7 Pemasangan, penetapan konfigurasi perkakasan WLAN dan ujian

Pemasangan boleh dibuat selepas selesai proses semakan dan penerimaan perkakasan. Pemasangan dilakukan berdasarkan lokasi yang telah ditetapkan sebelum ini. Seterusnya beberapa semakan dan ujian boleh dilakukan seperti senarai di bawah:

a. Semakan liputan hanya ke kawasan atau ruang pejabat yang diperlukan sahaja.
b. Pastikan liputan tidak sampai ke kawasan tidak sepatutnya. Contoh, kawasan perumahan bersebelahan.
c. Pastikan wayarles AP tanpa polisi tapisan tidak dipasang di dalam pusat data/bilik pelayan.
d. Semakan penggunaan saluran frekuensi dan *interference*.
e. Semakan penetapan lebar jalur.
f. Pengujian *onboarding* & capaian.
g. Semakan prestasi dengan ujian muat turun/naik, sidang video dan penstriman.
h. Penetapan prestasi asas (*baseline*).
i. Penetapan *threshold* & *alert*.
j. Semakan terhadap AP asing atau tidak sah (*rogue* AP).
k. Semakan *dashboard* pemantauan SLA/SLG.
l. Semakan janaan laporan.

5.3.8 Pengoptimuman

Pengoptimuman perlu dilakukan bagi memastikan objektif pelaksanaan WLAN dapat dicapai dan bagi memastikan WLAN dapat beroperasi dengan baik. Ia boleh dilakukan dengan menggunakan perisian WLC dan perisian perancangan/tinjauan wayarles. Antara semakan seterusnya yang boleh dilakukan adalah seperti berikut:

a. Pelaporan masalah.
b. Isyarat/pengawalan sumber tenaga(signal/*power gain control*).
c. Pengurusan sumber radio (*Radio Resource Management,* RRM).
d. *Wireless client load balancing*.
e. *Wireless Beacon Interval*.
f. *Sticky client*.
g. *Dynamic Multicast Optimization*.
h. Kadar ralat.
i. Penyesuaian semula konfigurasi (*tuning*).
j. Relokasi AP jika perlu.
k. Semakan pemantauan SLA/SLG.
l. Semakan kestabilan dan persediaan untuk UAT.

BAB 6: KESELAMATAN RANGKAIAN

6.1 Pengenalan

6.1.1 Kawalan keselamatan LAN adalah penting bagi memastikan kerahsiaan, integriti dan ketersediaan (*Confidentiality, Integrity and Availability*, CIA) maklumat kerajaan. Rangkaian LAN hendaklah dibangunkan dengan mengambil kira risiko pengubahsuaian, kebocoran dan kehilangan maklumat yang akan merugikan kerajaan. Pemilihan teknologi, perkakasan, perisian, konfigurasi dan prosedur operasi standard (SOP) yang betul adalah penting untuk menjamin CIA bagi 3 keadaan data iaitu data-dalam-simpanan (*data-at-rest*), data-dalam-pergerakan (*data-in-motion/transit*) dan data-yang-sedang-digunakan (*data-in-use*).

6.1.2 Bagi memastikan keselamatan rangkaian berada di tahap yang baik, setiap agensi perlu melihat dari sudut berikut:

a. Teknologi Perkakasan dan Perisian

i. NGFW bagi mengawal aliran trafik keluar masuk dan menghalang trafik luar yang tidak sah.

ii. Suis rangkaian melalui penggunaan VLAN bagi pembahagian (*segmentation*) rangkaian untuk pengasingan dan mengehadkan capaian.

iii. Peralatan NAC bagi mengawal dan memantau setiap pengguna yang diberikan kebenaran untuk mengguna pakai rangkaian termasuk penggunaan peralatan secara BYOD.

iv. Perisian antivirus atau anti *malware* terkini daripada sumber yang dipercayai.

v. Peralatan/perisian/perkhidmatan yang menyokong semakan reputasi alamat IP/nama domain dapat mencegah pengguna daripada

mengakses laman web berisiko dan membantu mencegah serangan yang menggunakan alamat IP/nama domain yang diambil alih oleh pihak yang tidak bertanggungjawab.

vi. Data log bagi tujuan analisis dan semakan.

vii. Penggunaan VPN untuk capaian secara *remote*.

viii. Penggunaan MFA untuk pengesahan akses peralatan/sistem pengurusan rangkaian.

ix. Kawalan titik integrasi rangkaian.

x. Menggunakan teknologi penyulitan WPA3 atau terkini untuk rangkaian wayarles.

xi. Mengehadkan liputan radio frekuensi rangkaian wayarles ke kawasan yang diperlukan sahaja.

xii. Kawalan keselamatan fizikal untuk akses ke bilik telekomunikasi dan peralatan rangkaian.

b. Manusia

i. Pelaksanaan latihan dan kempen kesedaran secara berkala bagi memastikan kakitangan sentiasa mendapat maklumat keselamatan terkini.

ii. Pentadbir rangkaian menggunakan protokol yang selamat untuk mengakses peralatan rangkaian melalui *Secure Shell/Secure Socket Shell* (SSH) atau *Hypertext Transfer Protocol Secure* (HTTPS) versi terkini.

iii. Menyahaktif dan tidak menggunakan servis/fungsi yang kurang selamat seperti Telnet dan *File Transfer Protocol* (FTP) yang tidak disulitkan.

iv. Pentadbir rangkaian menggunakan VLAN khusus bagi mengurus dan memantau peralatan rangkaian.

v. Tidak membuat capaian ke laman web yang tidak selamat dan mematuhi peraturan penggunaan rangkaian seperti dinyatakan dalam DKICT/PKS agensi.

c. Proses

i. Penyediaan Dokumen Keselamatan ICT agensi.

ii. Penyediaan PSP Agensi.

iii. Analisis kelemahan, ancaman, risiko dan kemungkinan.

iv. Melaksana, menguji dan menyelenggara peralatan secara berkala.

6.2 Pengurusan Keselamatan

6.2.1 Pengurusan Risiko Keselamatan Maklumat

a. Agensi perlu melaksana proses pengurusan risiko keselamatan maklumat secara berkala (sekurang-kurangnya sekali dalam setahun) berdasarkan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam yang dikeluarkan oleh Agensi Keselamatan Siber Negara (NACSA).

b. Sebarang risiko yang dikenal pasti ke atas perkakasan dan perisian rangkaian ICT yang boleh menjejaskan keselamatan maklumat kerajaan

hendaklah diambil tindakan kawalan yang sewajarnya berdasarkan nilai maklumat yang ingin dilindungi.

6.2.2 Pelan Pemulihan Bencana

Bagi tujuan ini, agensi hendaklah merujuk **Pekeliling Am Bilangan 1 Tahun 2025: Garis Panduan Pengurusan Kesinambungan Perkhidmatan dalam Perkhidmatan Awam *Business Continuity Management* (BCM)** yang menerangkan dan menyertakan templat strategi pemulihan bencana bermula dengan Analisis Impak Perkhidmatan sehingga pelan dan simulasi pemulihan bencana.

6.2.3 *Information Security Management System* (ISMS)

Perkhidmatan rangkaian yang menghubungkan pengguna dan sistem-sistem utama agensi disarankan untuk mendapat pensijilan ISMS.

6.2.4 Pensijilan Keselamatan Produk Rangkaian

Produk rangkaian yang mempunyai fungsi keselamatan hendaklah mendapat pensijilan keselamatan yang sesuai dan diiktiraf oleh kerajaan. Antara produk yang perlu mendapat pensijilan keselamatan ialah tembok keselamatan dan sistem penghalang pencerobohan (*Intrusion Prevention System*, IPS) yang perlu mendapat pensijilan keselamatan seperti *Evaluation Assurance Level* (EAL), *Common Criteria* dan lain-lain.

6.2.5 Mengenal Pasti Aset Rangkaian Yang Perlu Dilindungi

a. Perkakasan.
b. Perisian.
c. Data.

6.2.6 Mengenal Pasti Ancaman Keselamatan Rangkaian dan Perlindungan Yang Bersesuaian

Jenis-jenis ancaman keselamatan rangkaian dan perlindungannya:

a. Perisian hasad (*malware*):
Perlindungan - memasang perisian anti perisian hasad / antivirus, sentiasa mengemaskini sistem operasi/ *firmware* terkini, berhati-hati dengan lampiran e-mel dan muat turun dari laman web yang tidak dipercayai.

b. *Phishing*:
Perlindungan - Latih pengguna/ pentadbir rangkaian untuk mengenali e-mel *phishing* dan sahkan keaslian permintaan sebelum berkongsi maklumat sensitif.

c. *Ransomware*:
Perlindungan - Selalu sandarkan data penting secara berkala dan tetapkan kawalan akses yang kukuh untuk mengurangkan kesan serangan.

d. Serangan DoS/ DDoS:
Perlindungan - Gunakan perkhidmatan perlindungan DDoS dan pantau trafik rangkaian untuk mengesan anomali.

e. Akses tidak sah (*Unauthorized access*):
Perlindungan - Gunakan kawalan Identiti akses dan pengesahan pelbagai faktor.

f. Curi dengar (*Eavesdropping*) melalui penghiduan paket rangkaian:
Perlindungan - Pastikan data dan komunikasi rangkaian disulitkan contohnya penggunaan VPN/HTTPS/FTPS/SFTP.

g. *Spoofing*

i. Perlindungan *spoofing* alamat IP - Penggunaan tapisan paket melalui FW.

ii. Perlindungan *spoofing* alamat MAC - Pengesahan dua faktor untuk menguatkan keselamatan akses ke rangkaian. Kawalan akses fizikal memastikan hanya peranti yang sah yang dapat mengakses/ membuat sambungan ke perkakasan rangkaian. Pemantauan rangkaian untuk aktiviti mencurigakan dan perubahan alamat MAC. Penggunaan protokol anti *spoofing* seperti DHCP *snooping* dan *Dynamic* ARP *Inspection* (DAI);

h. *Man-In-The-Middle-Attack*:
Perlindungan - Pastikan sijil HTTPS pelayan adalah sah, data dan komunikasi disulitkan.

i. *Advanced Persistent Threat* (APT):
Perlindungan - Penggunaan FW dengan fungsi APT dan penilaian tahap keselamatan berkala.

6.2.7 Perlindungan Keselamatan Rangkaian Wayarles Bersesuaian

Bagi rujukan keselamatan dalam pembangunan dan pengoperasian rangkaian wayarles kawasan setempat, agensi disarankan untuk merujuk prinsip seperti yang digariskan dalam piawaian NIST SP 800-97 & 153. Selain itu, agensi juga boleh melaksanakan tetapan berikut bagi meningkatkan tahap keselamatan rangkaian wayarles:

a. Penetapan kata laluan kuat dan kawalan jangka hayat kata laluan.
b. Menggunakan piawaian WiFi *Protected Access* (WPA) 2/3 atau terkini.
c. Sijil pengguna atau pelayan untuk penyulitan.
d. Pengasingan segmen antara kakitangan agensi, tetamu dan perkakasan IoT.
e. Kawalan akses pengguna melalui pelaksanaan NAC.

f. Wayarles IPS (mengikut keperluan).
g. Semakan AP tidak sah.
h. Memastikan perisian (*firmware*) sentiasa dikemas kini.
i. Melaksanakan imbasan kelemahan keselamatan untuk perisian dan perkakasan wayarles.
j. Ujian pencerobohan dan prestasi.
k. Penambahbaikan konfigurasi.
l. Pemantauan keselamatan rangkaian wayarles berterusan.

Walau bagaimanapun, agensi adalah tertakluk dan perlu mematuhi akta, arahan dan pekeliling terkini berkaitan keselamatan yang dikeluarkan oleh NACSA dan Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) dari semasa ke semasa.

6.3 Reka Bentuk Keselamatan LAN

6.3.1 Berikut ialah elemen yang perlu ada dalam reka bentuk keselamatan LAN:

a. Membahagikan rangkaian berdasarkan tahap sensitiviti terhadap aset digital seperti:

   i. segmen luaran untuk Internet.
   ii. segmen DMZ untuk pelayan awam.
   iii. segmen dalaman untuk pelayan dalaman dan pengguna.

b. Memastikan keselamatan fizikal rangkaian seperti meletakkan peralatan rangkaian dalam rak dan suhu yang bersesuaian dan bilik yang berkunci.

c. Memastikan keselamatan logikal rangkaian dengan mewujud dan menguatkuasakan ACL atau tembok keselamatan di antara lokasi yang berbeza tahap sensitiviti terhadap aset digital.

d. Memperkukuh rangkaian dengan pengurusan *patch*, memasang perisian perlindungan *endpoint* dan hanya membenarkan *endpoint* yang telah dikenal pasti.

e. Agensi turut digalakkan menggunakan teknologi ATP sebagai mitigasi terhadap ancaman terkini yang lebih maju.

6.4 Penilaian Tahap Keselamatan LAN

6.4.1 Analisis kerentanan (*severity*) dalaman dan ujian penembusan perlu dilaksanakan secara berkala untuk menjamin bahawa LAN pengguna terkawal dengan baik dari peralatan *endpoint* seperti komputer, komputer riba, pelayan dan peranti LAN.

6.4.2 Untuk tujuan ini, agensi hendaklah merujuk pada **Surat Pekeliling Am Bilangan 4 Tahun 2024: Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam** bertarikh 21 Mac 2024 atau sebarang arahan Keselamatan yang berkuatkuasa.

6.5 Jaminan Operasi LAN

6.5.1 Pengauditan LAN

Agensi menggunakan kaedah atau alat yang bersesuaian untuk mengaudit rangkaian. Pengauditan penting bagi memudahkan pengurusan dan menjamin keselamatan rangkaian.

6.5.2 Pemantauan dan Analisis Log Aktiviti LAN

a. Pemantauan dan analisis log hendaklah dilaksanakan secara berkala bagi mengesan sebarang aktiviti yang mencurigakan. Pelaksanaan dan penggunaan aplikasi *Security Information and Event Management* (SIEM) adalah disarankan bagi mengesan sebarang aktiviti anomali secara masa nyata dalam rangkaian ICT yang berskala sederhana dan besar. Tempoh

penyimpanan log perlu dinyatakan di dalam DKICT/PKS agensi bagi membantu sebarang siasatan jika diperlukan.

b. Agensi di lokasi bersaiz kecil digalakkan untuk menyediakan kemudahan bagi menyimpan *event log*.

c. Untuk tujuan ini, semua peralatan rangkaian hendaklah menetapkan NTP yang sama bagi memastikan data berkenaan tarikh dan masa adalah direkodkan dengan tepat dan selaras. Agensi boleh merujuk kepada pihak SIRIM selaku jabatan yang menyelenggara Waktu Standard Malaysia.

6.5.3 **Kontrak Penyelenggaraan**

a. Kontrak penyelenggaraan bagi peralatan rangkaian boleh dilaksanakan dalam tempoh sekurang-kurangnya 3 tahun selepas perolehan.

b. Kontrak berkenaan hendaklah sekurang-kurangnya mengandungi perkara-perkara berikut:

i. Proses *escalation* bagi pengurusan masalah dan perubahan permintaan (*change request*).
ii. Perjanjian tahap perkhidmatan dengan sekurang-kurangnya 3 peringkat kerentanan berdasarkan keutamaan (*priority*) dengan penetapan masa tindakan (*response time*) dan masa penyelesaian (*resolution time*) yang diperlukan.
iii. Kenaan penalti yang sesuai jika penyedia perkhidmatan tidak memenuhi tahap perkhidmatan.

c. Mempertimbangkan langganan *Advanced Replacement* daripada pihak prinsipal serta peminjaman peralatan rangkaian (yang setaraf atau lebih baik) yang boleh disediakan oleh pihak pembekal perkhidmatan penyelenggaraan dalam tempoh pembaikan peralatan rangkaian yang rosak.

d. Mengenal pasti pembaharuan lesen peralatan yang diperlukan seperti tembok keselamatan untuk dimasukkan dalam skop perkhidmatan penyelenggaraan.

6.5.4 Pernyataan Dasar

Bagi memastikan keselamatan rangkaian ICT, agensi hendaklah mematuhi peraturan dan perundangan berkaitan keselamatan semasa yang berkuat kuasa merangkumi keselamatan rangkaian ICT yang mengandungi perkara seperti berikut:

a. Liputan dan fungsi peralatan rangkaian serta aspek keselamatan yang terlibat.
b. Kuasa dan tanggungjawab Bahagian/Unit yang menguruskan rangkaian agensi.
c. Peraturan penggunaan rangkaian berwayar.
d. Peraturan penggunaan rangkaian wayarles.

6.5.5 Prosedur Operasi Standard

a. Agensi hendaklah membangunkan Prosedur Operasi Standard (SOP) bagi setiap aktiviti yang atau proses rangkaian yang terlibat. Semua SOP juga perlu didokumenkan, dikemas kini dan dilaksanakan bagi memudahkan pemantauan tindakan.

b. Aktiviti yang sesuai dilaksanakan mengikut SOP adalah seperti berikut:

    i. Prosedur pengguna baru (seperti kakitangan baharu).
    ii. Prosedur aduan isu capaian rangkaian.
    iii. Prosedur permohonan perkhidmatan rangkaian.

c. Semua prosedur ini boleh dikonsolidasi dan diselaras dengan perkhidmatan ICT yang lain.

BAB 7: PENGURUSAN DAN PENGOPERASIAN LAN

7.1 Pengenalan

7.1.1 Pengurusan LAN yang baik dapat memastikan semua sumber rangkaian dapat digunakan dengan sepenuhnya dan menjamin kesinambungan operasi LAN di agensi. Pengurusan LAN ini merangkumi penyelenggaraan rangkaian, pemantauan perkakasan rangkaian, pelaporan status bulanan, pengemaskinian *firmware* dan *patches* serta pentadbiran pengguna. Manakala, pengoperasian LAN melibatkan kelancaran fungsi rangkaian, termasuk pemantauan aktiviti dengan cepat dan cekap bagi menangani dan menyelesaikan sebarang gangguan atau isu berkaitan LAN.

7.2 Peranan dan Tanggungjawab

7.2.1 Ketua Jabatan

Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut:

a. Memastikan pengguna memahami keperluan untuk membangun dan menguruskan LAN seperti yang dinyatakan dalam Garis Panduan Pembangunan dan Pengoperasian LAN Sektor Awam.

b. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) bagi mengurus dan mengoperasikan perkhidmatan LAN adalah mencukupi.

7.2.2 Ketua Pegawai Digital (*Chief Digital Officer*, CDO)

Peranan dan tanggungjawab CDO adalah seperti berikut:

a. Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan pengurusan dan pengoperasian LAN.

b. Menentukan keperluan pengurusan dan pengoperasian LAN bagi menambah baik perkhidmatan LAN kepada pengguna.

7.2.3 Pengurus ICT

Pengurus ICT ialah Pengarah Bahagian Teknologi Maklumat atau Ketua Seksyen Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a. Melaksanakan audit dan kajian semula keberkesanan perkhidmatan LAN di jabatan dari semasa ke semasa berdasarkan perubahan teknologi terkini dan keperluan pengguna.

b. Melaporkan mengenai prestasi perkhidmatan LAN secara berkala kepada CDO.

c. Memastikan persekitaran LAN adalah selamat dan diyakini untuk digunakan oleh pengguna.

7.2.4 Pentadbir Rangkaian

Peranan dan tanggungjawab pentadbir rangkaian adalah seperti berikut:

a. Menganalisis keperluan dan cadangan reka bentuk LAN di agensi.

b. Membuat pemasangan dan konfigurasi peralatan rangkaian berdasarkan keperluan dan cadangan reka bentuk LAN yang dipersetujui.

c. Menyediakan dokumentasi keperluan rangkaian yang mengandungi maklumat berikut:

   i. gambar rajah tapak dengan perincian susun atur LAN dan persekitaran bangunan termasuk penempatan ruang kerja, keperluan sumber elektrik, sistem penyejukan, sistem pencegah kebakaran,

lokasi peralatan rangkaian, sistem pengkabelan, penempatan talian telefon dan sebagainya.

ii. maklumat dan konfigurasi pemasangan aset dan perisian rangkaian.

iii. reka bentuk logikal dan reka bentuk fizikal rangkaian.

d. Melindungi persekitaran LAN daripada sebarang ancaman keselamatan menggunakan kawalan keselamatan yang bersesuaian.

e. Memantau prestasi dan menambahbaik perkhidmatan LAN sekiranya perlu.

f. Memastikan komponen rangkaian adalah mencukupi dan dapat menampung keperluan perkhidmatan LAN.

g. Memastikan komponen rangkaian beroperasi dengan baik dan optimum.

h. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta.

i. Memantau laluan trafik LAN dari semasa ke semasa dan mengambil tindakan dengan segera sekiranya berlaku kesesakan trafik rangkaian atau LAN tidak dapat beroperasi dengan baik.

7.2.5 **Meja Bantuan**

Agensi perlu menyediakan saluran bagi aduan LAN. Pengguna yang menghadapi masalah menggunakan perkhidmatan LAN boleh menghubungi meja bantuan untuk mendapatkan bantuan dengan segera.

7.2.6 Pengguna

Peranan dan tanggungjawab pengguna seperti berikut:

a. Membaca, memahami dan mematuhi amalan-amalan terbaik dalam garis panduan ini.

b. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengurus ICT atau pentadbir rangkaian dengan segera.

7.2.7 Pihak Ketiga (Pembekal, Kontraktor dan lain-lain)

Peranan dan tanggungjawab pihak ketiga adalah seperti berikut:

a. Membaca, memahami dan mematuhi garis panduan ini.

b. Memberikan khidmat sokongan teknikal bagi menyelesaikan isu atau gangguan perkhidmatan LAN.

c. Menjaga kerahsiaan maklumat berkaitan perkhidmatan LAN di jabatan termasuk konfigurasi peralatan rangkaian serta maklumat IP.

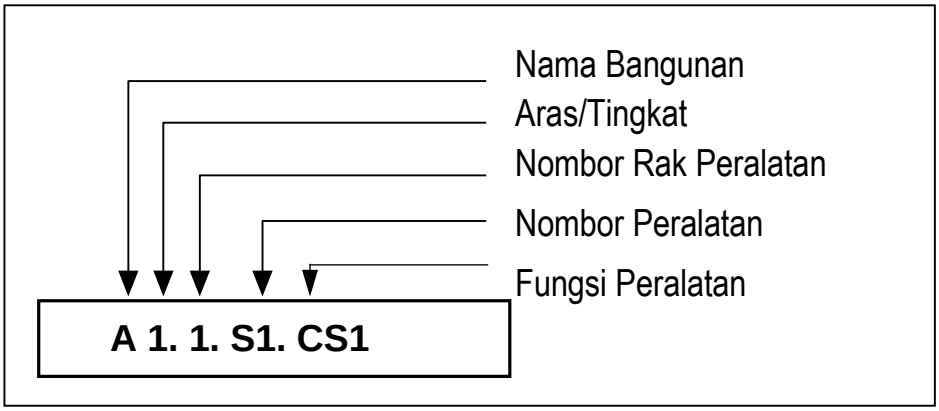
7.3 Pengurusan Operasi LAN

7.3.1 Konfigurasi LAN

Konfigurasi LAN membolehkan pentadbir rangkaian membangunkan rangkaian untuk menyokong komunikasi rangkaian di agensi. Konfigurasi/tetapan nama/label mesti logik dan konsisten. Setiap elemen fizikal (ruang, kabinet, rak, *patch panel, port,* kabel) mesti dikenal pasti dengan pengecam unik. Antara tetapan yang terlibat adalah:

a. **Tetapan nama/pelabelan peralatan rangkaian**

Semua peralatan rangkaian hendaklah diberi nama dan dilabel memudahkan proses pengecaman peralatan. Sistem pelabelan yang digunakan adalah mengikut lokasi serta fungsi peralatan seperti di Rajah 7.1 berikut:



Rajah 7.1: Tetapan Nama/ Pelabelan bagi Peralatan Rangkaian

Panduan

“A” merujuk kepada nama bangunan. Contoh: Blok A.

“1” merujuk kepada aras/tingkat. Contoh: Aras 1.

“1” merujuk kepada nombor rak peralatan rangkaian tersebut ditempatkan. Contoh: Rak Peralatan Rangkaian Nombor 1.

“S1” merujuk kepada nombor peralatan di dalam rak tersebut.

Contoh: Suis Nombor 1

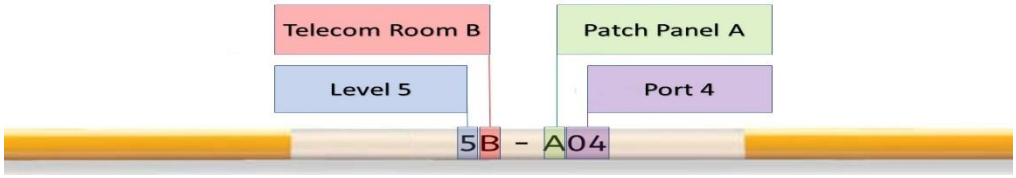
“CS1” merujuk kepada fungsi peralatan di dalam rak tersebut.

Contoh: *Core Switch* nombor 1

Manakala bagi pelabelan fizikal, ia mesti mudah dibaca dan tahan lama. Setiap kabel dan laluan mesti dilabel dengan maklumat yang konsisten (menggunakan aksara *alphanumeric*). Pada sambungan seperti *patch panel, outlet,* atau penamatan kabel. Label boleh dipaparkan di muka panel atau pada permukaan peranti lain. Semua label hendaklah dihasilkan melalui peranti pencetak (bukan tulisan tangan) untuk memastikan hasil yang konsisten dan mudah dibaca. Label mesti tahan terhadap faktor persekitaran (contoh: haba, kelembapan, sinaran UV) serta tidak mudah tertanggal.

Semua maklumat label harus direkod dalam sistem pengurusan infrastruktur kabel (boleh menggunakan sistem *spreadsheet* atau perisian khusus) yang menyatakan maklumat seperti lokasi, jenis kabel, jenis sambungan dan tarikh pemasangan. Rekod ini hendaklah dikemas kini setiap kali berlaku perubahan untuk memastikan data yang tepat bagi rujukan pada masa hadapan. Standard **TIA 606** boleh dijadikan rujukan lanjut.

b. **Tetapan nama/pelabelan kabel rangkaian**



Rajah 7.2: Tetapan Nama/Pelabelan Kabel Rangkaian

Pelabelan bagi kabel hendaklah dipasang secara kekal pada kedua-dua hujung kabel, biasanya dalam jarak 30 cm (12 inci) dari hujung penebat kabel (Rujuk Rajah 7.2).

c. **Tetapan konfigurasi penghala**

Menentukan tetapan laluan yang betul antara rangkaian.

d. **Tetapan konfigurasi hos**

Menyediakan sambungan rangkaian pada komputer hos/komputer riba dengan tetapan rangkaian seperti alamat IP, proksi, nama rangkaian dan ID/kata laluan, untuk membolehkan sambungan rangkaian dan komunikasi dilaksanakan.

e. **Tetapan konfigurasi perisian**

i. Pentadbir rangkaian di agensi hendaklah mengurus maklumat mengenai semua komponen rangkaian komputer dengan baik dan teratur menggunakan *Configuration Management Database* (CMDB).

ii. Pangkalan data ini mengandungi maklumat lokasi dan alamat IP semua peralatan, termasuk maklumat tentang tetapan lalai, program, versi dan kemas kini yang dipasang dalam komputer rangkaian.

iii. Sekiranya rangkaian memerlukan tindakan penambahbaikan (*repair*), pengubahsuaian (*modification*) atau peningkatan, pentadbir rangkaian akan merujuk kepada CMDB untuk menentukan tindakan terbaik.

7.3.2 **Migrasi**

Selepas beberapa tempoh pengoperasian rangkaian di agensi, akan terdapat keperluan bagi agensi untuk melaksanakan migrasi terhadap infrastruktur rangkaian sedia ada disebabkan oleh perkara-perkara berikut:

a. Penggunaan peralatan rangkaian yang baharu disebabkan peralatan yang digunakan sama ada telah *End of Life* (EOL) atau EOS.

b. Integrasi rangkaian.

c. Keperluan agensi terhadap perkhidmatan baharu.

d. Perubahan teknologi rangkaian yang baharu seperti teknologi *converged network* dengan suara, video dan trafik data disebabkan teknologi lama tidak lagi dapat menyokong atau menampung keperluan rangkaian semasa.

e. Pembaharuan perkakasan (*refresh hardware*) yang mengambil kira ciri-ciri dan tambahan kapasiti baharu.

f. Perubahan struktur IP baru.

g. Proses migrasi LAN hendaklah dilaksanakan mengikut proses dan prosedur yang ditetapkan bagi menjamin kejayaan migrasi.

7.3.3 **Pemantauan Rangkaian**

a. Pemantauan rangkaian secara 24 jam setiap hari ialah proses kritikal dalam memastikan kestabilan, keselamatan dan kecekapan infrastruktur ICT agensi Sektor Awam. Ia membolehkan pengesanan awal terhadap masalah seperti gangguan sambungan, kelewatan penghantaran data, atau potensi serangan keselamatan, sekali gus membantu dalam pengurusan dan penyelenggaraan sistem rangkaian secara proaktif. Bahagian Pengurusan Maklumat adalah bertanggungjawab dalam melaksanakan pemantauan rangkaian tersebut sama ada menggunakan kaedah metrik ukuran atau alat pemantauan rangkaian. Antara metrik ukuran yang perlu/boleh dipantau adalah seperti berikut:

i. Ketersediaan – *uptime, downtime* dan *mean time to repair* (MTTR).
ii. Prestasi - *bandwidth utilization, jitter, latency, packet loss* dan *throughput.*
iii. Keselamatan - *access to non productive sites/ command & control* (C&C), *intrusion/advanced persistent threat, failed login attempts* dan *incident response time.*

Alat pemantauan yang bersesuaian dan boleh digunakan bagi memastikan perkhidmatan LAN agensi beroperasi secara berkesan dan berterusan adalah seperti berikut:

i. **Pemantauan Melalui Perisian Perkakasan Rangkaian**

- LAN boleh dilakukan dengan menggunakan perisian untuk mengurus perkakasan rangkaian. Contohnya, perisian pengurusan IPS, perisian pengurusan tembok keselamatan, perisian suis rangkaian atau melalui perisian penganalisis trafik rangkaian. Maklumat sumber pemprosesan, memori, storan, penggunaan lebar jalur, trafik rangkaian yang disekat dan maklumat mengikut fungsi perkakasan rangkaian dapat dipantau melalui perisian pengurusan perkakasan tersebut.

- Pemantauan *visibility* trafik rangkaian atau keboleh lihatan data trafik rangkaian juga akan dapat membantu mengoptimumkan pengoperasian rangkaian harian. Bacaan keadaan trafik rangkaian daripada data telemetri perkakasan rangkaian harian normal boleh dijadikan asas analisis perbandingan bagi mengenal pasti keadaan trafik rangkaian luar jangka untuk tindakan susulan. Tetapan ambang rangkaian (*network threshold*) juga boleh dibuat bagi memberi amaran awal dalam melaksanakan pemantauan dan mengelak isu dijangka timbul dengan lebih proaktif.

- Pemantauan juga dibuat dengan melaksanakan ujian imbasan kelemahan dan ujian penembusan rangkaian seterusnya melaksanakan penilaian prestasi rangkaian bagi memastikan rangkaian beroperasi di tahap yang diperlukan.

ii. **Sistem Pemantauan Rangkaian (*Network Management System*, NMS)**

- Setiap agensi yang mempunyai reka bentuk LAN dalam kategori besar dan kategori kampus, digalakkan menggunakan NMS bagi memudahkan pemantauan ke atas LAN daripada segi ketersediaan dan keseluruhan prestasi hos dan perkhidmatan rangkaian. NMS membolehkan pentadbir rangkaian mengesan dan melaporkan kegagalan peralatan atau sambungan rangkaian. Selain itu, NMS mengukur penggunaan CPU pada hos, penggunaan lebar jalur rangkaian dan lain-lain aspek operasi.

- Pentadbir rangkaian akan menerima notifikasi sama ada melalui pelayan pengurusan rangkaian, e-mel atau talian telefon apabila berlaku kegagalan seperti respon daripada peralatan rangkaian terlalu perlahan (*unacceptable slow response*) atau tingkah laku yang tidak dijangka (*unexpected behaviour*).

- Agensi mempunyai pilihan untuk menggunakan peralatan perisian pemantauan rangkaian (*network management tools software*) komersial atau sumber terbuka. Pemilihan peralatan tersebut bergantung kepada fungsi atau ciri-ciri pemantauan yang perlu dilaksanakan dan juga peruntukan kewangan agensi.

b. **Pusat Operasi Rangkaian (*Network Operation Centre*, NOC)**

i. NOC merupakan sebuah fasiliti atau pusat kawalan yang bertanggungjawab untuk memantau, mengurus dan menyelenggara sistem rangkaian dan infrastruktur ICT secara berterusan.

ii. Agensi yang mempunyai reka bentuk LAN yang besar dan persekitaran rangkaian kompleks atau mempunyai rangkaian besar multi lokasi memerlukan ciri-ciri keselamatan dan kadar ketersediaan operasi yang tinggi digalakkan untuk melaksanakan aktiviti pemantauan dan perkhidmatan sokongan keseluruhan rangkaian melalui NOC.

c. **Laporan Pemantauan**

i. Laporan pemantauan hendaklah disediakan sekurang-kurangnya sekali dalam tempoh sebulan tertakluk kepada keperluan jabatan atau agensi. Laporan ini membolehkan pihak pengurusan mendapat maklumat mengenai LAN agensi termasuk penggunaan jalur lebar, ketersediaan peralatan rangkaian dan aktiviti capaian pengguna.

ii. Sekiranya berlaku penyalahgunaan terhadap LAN seperti capaian ke laman web yang tidak dibenarkan, konfigurasi sistem dan penggunaan perisian yang tidak mematuhi piawaian, tindakan hendaklah diambil berdasarkan DKICT/PKS agensi.

7.3.4 *Troubleshooting*

a. Pentadbir rangkaian atau pegawai sokongan rangkaian bertanggungjawab untuk memulih dan menstabilkan LAN sekiranya terdapat isu atau berlaku gangguan terhadap perkhidmatan LAN di agensi.

b. Langkah-langkah amalan terbaik untuk menyelesaikan masalah LAN adalah:

i. Mengenal pasti isu atau masalah sebenar.
ii. Mengasingkan punca masalah.
iii. Merangka kaedah penyelesaian masalah.
iv. Melaksanakan pelan penyelesaian masalah.
v. Membuat pengujian untuk mengesahkan bahawa masalah telah diselesaikan.
vi. Mendokumenkan masalah dan penyelesaian.
vii. Menyediakan maklum balas kepada pengguna.

7.3.5 **Sandaran Data**

a. Pentadbir rangkaian bertanggungjawab memastikan proses sandaran data konfigurasi peralatan rangkaian dilaksanakan secara berkala, teratur dan selamat bagi menjamin ketersediaan data, meminimumkan kegagalan perkhidmatan rangkaian serta mempercepatkan proses pemulihan sekiranya berlaku sebarang insiden seperti kerosakan peranti, serangan siber atau bencana alam.

b. Peranan pentadbir rangkaian dalam melaksanakan penduaan maklumat konfigurasi rangkaian mematuhi perkara-perkara berikut:

i. Membuat sandaran secara berkala atau sekurang-kurangnya sekali atau setiap kali berlaku perubahan konfigurasi.
ii. Membuat penyulitan data ke atas konfigurasi sandaran untuk melindungi kerahsiaan.

iii. Menguji sistem sandaran bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.
iv. Menyimpan sekurang-kurangnya 3 generasi/versi sandaran.
v. Merekod dan menyimpan salinan sandaran di lokasi yang selamat daripada ancaman fizikal dan siber.
vi. Memantau proses salinan sandaran secara berkala.

7.3.6 **Penyelenggaraan**

Penyelenggaraan meliputi aktiviti menyelenggara peralatan rangkaian seperti tembok keselamatan, BMT, IPS, CF, penghala, pelayan DNS, DHCP dan AD/ LDAP. Pentadbir rangkaian hendaklah memastikan perkara berikut dipatuhi:

a. Semua peralatan rangkaian yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar.

b. Peralatan rangkaian hanya boleh diselenggara oleh pegawai di agensi masing-masing atau pihak ketiga yang dibenarkan sahaja.

c. Bertanggungjawab terhadap setiap peralatan rangkaian bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan.

d. Menyemak dan menguji semua peralatan rangkaian sebelum dan selepas proses penyelenggaraan.

e. Memaklumkan kepada pengguna mengenai jadual penyelenggaraan yang telah ditetapkan.

f. Menyimpan rekod penyelenggaraan.

7.3.7 **Dokumentasi**

a. Pengurusan dokumentasi LAN yang teratur dan kemas amat penting sebagai rujukan kepada pentadbir rangkaian sekiranya berlaku masalah pada perkhidmatan LAN terutamanya bagi agensi yang mempunyai LAN yang besar dan kompleks.

b. Perkara yang perlu didokumentasi adalah:

   i. Alamat IP.
   ii. Tetapan konfigurasi.
   iii. Rajah topologi.
   iv. Rekod pengkabelan.
   v. Spesifikasi.
   vi. Perkhidmatan rangkaian.

c. Pentadbir rangkaian perlu menyediakan dokumentasi dalam 2 bentuk iaitu:

   i. Salinan elektronik yang mudah dikemas kini sekiranya berlaku perubahan konfigurasi.
   ii. Salinan keras disimpan di lokasi yang selamat.

d. Dokumentasi perlu dikemas kini setiap kali berlaku perubahan dalam rangkaian.

BAB 8: SENARAI PIAWAIAN/STANDARD

8.1 Senarai Piawaian/Standard

Agensi hendaklah memastikan perancangan, pembangunan dan pengoperasian mengambil kira garis panduan dan piawaian/standard yang sedang berkuatkuasa (tidak terhad kepada) seperti Jadual 8.1.

Jadual 8.1 Senarai Piawaian/Standard

STANDARD	PENERANGAN
IEEE 802.3	Piawaian asas untuk rangkaian berwayar/Ethernet
IEEE 802.11	Piawaian asas untuk rangkaian Wayarles
IEEE 802.1X	Kawalan Akses Rangkaian berdasarkan *port*
IEEE 802.3 af/at/bt	Kuasa Elektrik melalui Ethernet/*Power over Ethernet* (PoE/PoE+/PoE++)
TIA-568	Penetapan keperluan untuk pendawaian berstruktur dalam bangunan, termasuk jenis kabel
TIA-606	Penetapan skim label dan dokumentasi untuk infrastruktur telekomunikasi
NIST SP 800-153	Pembangunan rangkaian wayarles dengan tahap keselamatan kukuh
UL 969	Penandaan dan label

Lampiran A1

SENARAI SEMAK KEPERLUAN MINIMUM PEMBANGUNAN DAN PENGOPERASIAN LAN SEKTOR AWAM

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
1.	**UMUM**				
	(i) Contoh lokasi	Klinik Desa	Klinik Kesihatan	Kementerian Kerja Raya	PCN / Kampus
	(ii) Persediaan tapak a) Rak rangkaian b) Bekalan kuasa c) Pengkabelan d) Persekitaran kondusif	√	√	√	√
	(iii) Rangkaian Kawasan Setempat (LAN) *Backbone*	1 Gbps	10 Gbps	10 Gbps	multi 10 Gbps
	(iv) Rangkaian Kawasan Luas (WAN) /*Internet Speed* (Minimum)	1 Mbps[1]	10 Mbps[1]	100 Mbps	1 Gbps
	(v) Alamat IP (IPv4 & IPv6)	√	√	√	√

[1] Tertakluk kepada ketersediaan teknologi rangkaian di lokasi

Lampiran A1

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
2.	**REKA BENTUK RANGKAIAN**				
	(i) Reka bentuk hierarki (Lapisan teras dan lapisan akses)	-	√	-	-
	(ii) Reka bentuk hierarki (Lapisan teras, lapisan pengagihan dan lapisan akses)	-	-	√	√
	(iii) Ketersediaan tinggi (melibatkan lapisan teras dan lapisan pengagihan)	-	-	√	√
	(iv) Pelbagai agensi	-	-	-	√
3.	**KONFIGURASI**				
	(i) *Quality of Service* (QoS)	*Tertakluk kepada keperluan agensi*			
	(ii) *Link Aggregation Control Protocol* (LACP)	-	*Tertakluk kepada keperluan agensi*		
	(iii) *Network Time Protocol* (NTP)	-	√	√	√

Lampiran A1

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
	(iv) *Virtual Local Area Network* (VLAN)	-	√	√	√
4.	**TEKNOLOGI YANG MENYOKONG PERKHIDMATAN AGENSI**				
	(i) *Voice over IP* (VoIP)	√	√	√	√
	(ii) *Video Conferencing*	√	√	√	√
	(iii) Internet Benda *(Internet of Things* atau IoT*)*	*Tertakluk kepada keperluan agensi*			
	(iv) *Software-Defined Networking* (SDN)	*Tertakluk kepada keperluan agensi*			
	(v) Platfom yang menyokong *Network Function Virtualization* (NFV)	*Tertakluk kepada keperluan agensi*			
	(vi) *Closed-Circuit Television* (CCTV)	*Tertakluk kepada keperluan agensi*			
5.	**PERALATAN/PERISIAN/FUNGSI RANGKAIAN**				
	(i) Talian Internet dan penghala oleh Pembekal	√	√	√	√

Lampiran A1

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
	Khidmat Internet (*Internet Service Provider*, ISP)				
(ii)	Tembok Keselamatan (*Firewall*)	*Tertakluk kepada keperluan agensi*	√	√	√
(iii)	Sistem Pengesanan Pencerobohan (*Intrusion Detection System*)	*Tertakluk kepada keperluan agensi*	√	√	√
(iv)	Web URL/ *Content Filtering* (CF)	*Tertakluk kepada keperluan agensi*		√	√
(v)	*Bandwidth Management Tool* (BMT)	-	√	√	√
(vi)	Pengawal Wayarles LAN	-	√	√	√
(vii)	Wayarles *Access Point*	*Tertakluk kepada keperluan agensi*	√	√	√
(viii)	*Power over Ethernet* (PoE) *Switch*	-	*Tertakluk kepada keperluan agensi*	√	√
(ix)	*Uninterruptible Power Supply* (UPS)	*Tertakluk kepada keperluan agensi*			

Lampiran A1

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
(x)	Sistem Pemantauan Rangkaian (*Network Monitoring System*, NMS)	-	*Tertakluk kepada keperluan agensi*	√	√
(xi)	Sistem Penghalang Pencerobohan Wayarles(*Wireless Intrusion Prevention System,* WIPS)	-	*Tertakluk kepada keperluan agensi*		
(xii)	*Advanced Threat Protection* (ATP)	-	*Tertakluk kepada keperluan agensi*		√
(xiii)	Kawalan akses melalui *Active Directory* (AD)/ *Lightweight Directory Access Protocol* (LDAP)	-	√	√	√
(xiv)	Sistem Nama Domain (*Domain Name System*, DNS)	-	√	√	√
(xv)	*Dynamic Host Configuration Protocol* (DHCP)	√	√	√	√

Lampiran A1

No	Perkara	Kategori Rangkaian			
		Kecil (1 hingga 24 *port* rangkaian)	**Sederhana (25 hingga 100 *port* rangkaian)**	**Besar (melebihi 100 *port* rangkaian)**	**Kampus (multi lokasi, multi agensi)**
(xvi)	*Security Operations Center* (SOC) dan *Network Operations Center* (NOC)	-	*Tertakluk kepada keperluan agensi*		√
(xvii)	*Network Security Analytics*	-	*Tertakluk kepada keperluan agensi*		√
(xviii)	*Secured Communication* (TLS, VPN, IPSec dan lain-lain)	√	√	√	√
(xix)	*Event log* atau *Audit trail*	*Tertakluk kepada keperluan agensi*			√
(xx)	*Single Sign-On* (SSO)	*Tertakluk kepada keperluan agensi*			
(xxi)	*Multihoming Internet*	-	-	-	√

Lampiran A2

[CONTOH] SENARAI SEMAK PENGUJIAN RANGKAIAN

KEMENTERIAN/JABATAN:_____

FASA	PERKARA	KRITERIA PENGUJIAN	STATUS	CATATAN / ISU	TINDAKAN
UAT	Latihan Pengguna Akhir	Pengguna diberi panduan tentang cara menggunakan rangkaian			
	Keselamatan	SPA telah selesai dilaksanakan			
		Pengguna hanya boleh akses data atau modul mengikut peranan			
		Semua capaian berwayar dan wayarles disulitkan			
		Signal wayarles (*heat map*) hanya untuk kawasan diperlukan sahaja			
	Fungsi sistem	Semua perkhidmatan/fungsi sistem pengurusan rangkaian beroperasi mengikut spesifikasi			
	Senario sebenar	Skrip pengujian berdasarkan aliran kerja sebenar pengguna			
	Kebolehgunaan	Antaramuka jelas dan mesra pengguna serta boleh diakses			
	Integrasi	Sistem berjaya berintegrasi dengan sistem lain (SSO, AD, LDAP, API, ID Digital, WLC dll)			
	Simulasi Pengguna	Pengujian pemindahan fail besar tanpa gangguan			
		Capaian Aplikasi, cetakan, komunikasi antara peranti			
		Persidangan video			
		Penstriman video masa nyata			
		Capai ke/dari Internet			
	Prestasi Rangkaian	Masa tindak balas capaian, kehilangan paket, *latency* dan *throughput* diuji berdasarkan tetapan *Quality of Service*			

Lampiran A2

FASA	PERKARA	KRITERIA PENGUJIAN	STATUS	CATATAN / ISU	TINDAKAN
		(QoS) oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) atau berdasarkan standard amalan terbaik			
	Medium rangkaian	Semua pengujian dilaksanakan melalui medium rangkaian berwayar dan wayarles			
	Penyelesaian Isu	Semua isu kritikal telah diatasi			
	Laporan UAT	Hasil pengujian, isu dan cadangan penambahbaikan perlu direkodkan			
	Kelulusan pengguna	Pengguna mengesahkan ujian penerimaan UAT			
PAT	Pemasangan lengkap	Semua perkakasan dipasang & berlabel dengan betul			
	Konfigurasi sistem	IP, VLAN, *firewall*, NAT, DNS, WLC dikonfigurasikan mengikut spesifikasi			
	Pengujian teknikal	Skrip pengujian sambungan LAN/WAN diuji			
	Fungsi *Redundancy* Rangkaian	Sambungan ketersediaan tinggi (HA), *failover* dan komunikasi antara bangunan/ agensi berfungsi			
	Ketahanan Sistem	Pengujian beban maksimum rangkaian (contoh: sambungan/simulasi capaian 200 peranti secara serentak dari pelbagai lokasi)			
	Kestabilan awal sistem	Sistem stabil ≥ 48 jam (bergantung kontrak)			
	Keselamatan	Pengujian keselamatan kerentanan **horizontal** antara agensi. Hanya *port* diperlukan sahaja dibuka. Perkongsian *file/folder Peer to Peer* (P2P) berisiko perlu disekat			
		Pengujian keselamatan kerentanan **vertrikal** ke/dari Internet. Hanya *port* diperlukan sahaja dibuka. Perkongsian *file/folder Peer to Peer* (P2P) berisiko perlu disekat. Ujian capaian ke *virus/malware test file*			
		Polisi kawalan akaun pengguna dan Autentikasi Multi-Faktor (MFA)			

Lampiran A2

FASA	PERKARA	KRITERIA PENGUJIAN	STATUS	CATATAN / ISU	TINDAKAN
		Pengasingan peranti/komputer pengguna bermasaalah			
		Analisa log capaian dan tempoh simpanan berdasarkan arahan/ pekeliling berkaitan keselamatan			
	Medium rangkaian	Semua pengujian dilaksanakan melalui medium rangkaian berwayar dan wayarles			
	Penyelesaian Isu	Semua isu kritikal telah diatasi			
	Laporan PAT	Hasil pengujian, isu dan cadangan penambahbaikan perlu direkodkan			
	Kelulusan pengguna	Pengguna mengesahkan ujian penerimaan PAT			
FAT	Integrasi Komponen	Semua keseluruhan komponen berfungsi bersama tanpa masalah dan stabil bagi tempoh 1-3 bulan			
	Pengujian Kegagalan	Pengujian dalam situasi kegagalan perkakasan/perisian teras rangkaian (contoh: bekalan elektrik terputus dan kesan terhadap perkakasan *core switch* & WLC)			
	Keselamatan	Audit konfigurasi - Semakan semula konfigurasi akhir & keselamatan			
	Prestasi Rangkaian	Masa tindak balas capaian, kehilangan paket, *latency* dan *throughput* diuji berdasarkan tetapan *Quality of Service* (QoS) oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) atau berdasarkan standard amalan terbaik			
		Pengurusan pemantauan rangkaian keseluruhan, analisa janaan laporan keseluruhan dan pengurusan insiden/ masaalah capaian			
		Analisa prestasi *baseline* untuk tetapan keperluan kapasiti tambahan akan datang			
	Medium rangkaian	Semua pengujian dilaksanakan melalui medium rangkaian berwayar dan wayarles			
	Penyelesaian Isu	Semua isu kritikal telah diatasi			

Lampiran A2

FASA	PERKARA	KRITERIA PENGUJIAN	STATUS	CATATAN / ISU	TINDAKAN
	Laporan FAT	Laporan lengkap termasuk hasil ujian keselamatan rangkaian, prestasi capaian dan dokumen penyerahan semua *deliverables* disediakan			
	Pengesahan Pengguna	Pengguna mengesahkan ujian penerimaan akhir			