# PEKELILING NAIB CANSELOR

## Bilangan 04 Tahun 2025

## GARIS PANDUAN PENGGUNAAN RANGKAIAN UNIVERSITI TEKNOLOGI MARA (UiTM)

### TUJUAN

1. Pekeliling ini bertujuan untuk memaklumkan kepada semua staf Universiti berkenaan pelaksanaan Garis Panduan Penggunaan Rangkaian Universiti Teknologi MARA (UiTM).

### LATAR BELAKANG

2. Garis Panduan Penggunaan Rangkaian UiTM digubal bagi menyatakan peranan dan tanggungjawab semua pengguna perkhidmatan rangkaian yang disediakan oleh UiTM.

3. Majlis Eksekutif Universiti (MEU) di dalam mesyuarat bil. 02 / 2025 pada 15 Januari 2025 telah meluluskan pelaksanaan Garis Panduan Penggunaan Rangkaian Universiti Teknologi MARA (UiTM).

### PELAKSANAAN

4. Garis panduan ini meliputi prosedur penggunaan perkhidmatan sistem rangkaian UiTM bagi semua jenis peralatan komunikasi data sama ada berwayar atau tanpa wayar yang bersambung ke sistem rangkaian UiTM. Garis panduan ini juga meliputi aspek keselamatan sistem rangkaian UiTM seperti yang dinyatakan dalam "Garis Panduan Penggunaan Rangkaian UiTM" pada Lampiran A.

5. Objektif garis panduan ini adalah seperti berikut:

5.1 Menjelaskan tentang penyediaan perkhidmatan rangkaian UiTM;

5.2 Memastikan keselamatan rangkaian UiTM terjamin; dan

5.3 Mengelakkan gangguan akses ke sistem rangkaian UiTM.

**TARIKH DIKELUARKAN**

6. Pekeliling dikeluarkan pada 20 Mei 2025.

**TARIKH KUAT KUASA**

7. Pekeliling ini berkuat kuasa mulai daripada tarikh ia dikeluarkan.

8. **Dengan berkuat kuasanya pekeliling ini, Garis Panduan Penggunaan Rangkaian UiTM bil. 03 / 2022 adalah dibatalkan.**

**PEMAKAIAN**

9. Pekeliling ini adalah terpakai kepada semua staf Universiti Teknologi MARA.

اوسها، تقوى، موليا

**"MALAYSIA MADANI"**

**"BERKHIDMAT UNTUK NEGARA"**

**(PROFESOR DATUK Ts. DR. SHAHRIN BIN SAHIB @ SAHIBUDDIN, FASc)**
Naib Canselor

UNIVERSITI TEKNOLOGI MARA

# GARIS PANDUAN PENGGUNAAN RANGKAIAN UNIVERSITI TEKNOLOGI MARA (UiTM)

# KANDUNGAN

# 1. PENGENALAN

## 1.1 TUJUAN

Garis Panduan ini disediakan oleh Jabatan Digital UiTM bertujuan sebagai panduan umum kepada semua pengguna perkhidmatan rangkaian yang disediakan oleh UiTM. Perkhidmatan rangkaian ini termasuk rangkaian berwayar, rangkaian tanpa wayar (WiFi) dan *Wide Area Network* (WAN). Mana-mana garis panduan terperinci berkaitan perkhidmatan rangkaian hendaklah dibaca bersama dengan garis panduan umum ini.

## 1.2 OBJEKTIF

Objektif Garis panduan ini adalah untuk:

(a) Menjelaskan tentang penyediaan perkhidmatan rangkaian UiTM;
(b) Memastikan keselamatan rangkaian UiTM terjamin; dan
(c) Mengelakkan gangguan akses ke sistem rangkaian UiTM.

## 1.3 SKOP

Garis Panduan perkhidmatan rangkaian UiTM merangkumi perkhidmatan sistem rangkaian UiTM bagi semua jenis peralatan komunikasi data berwayar atau tanpa wayar yang bersambung ke rangkaian UiTM dan keselamatan sistem rangkaian UiTM.

## 1.4 AKRONIM DAN TAKRIFAN

Akronim dan takrifan yang digunakan dalam Garis Panduan ini, melainkan jika konteksnya menghendaki makna yang lain.

| AKRONIM | DEFINISI |
|---|---|
| BYOD | *Bring Your Own Device* |
| DHCP | *Dynamic Host Configuration Protocol* |
| DNS | *Domain Name System* |
| ICT | *Information and Communication Technology* |
| IP | *Internet Protocol* |
| LAN | *Local Area Network* |
| PTj | Pusat Tanggungjawab |
| P2P | *Peer-to-Peer* |
| SLA | *Service Level Agreement* |
| SSID | *Service Set Identifier* |
| UiTM | Universiti Teknologi MARA |
| VPN | *Virtual Private Network* |
| WAN | *Wide Area Network* |

| TAKRIFAN | DEFINISI |
|---|---|
| *Firewall* | Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya. |
| *Internet* | Sistem rangkaian komunikasi global. Ia merangkumi Infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer. Internet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian. |
| *Internet of Things* (IoT) | Peranti dengan keupayaan memproses, berhubung dan bertukar data dengan peranti atau sistem lain melalui Internet atau rangkaian komunikasi lain. |
| Pihak ketiga | Pihak yang membekalkan atau menerima perkhidmatan kepada atau daripada UiTM. Mereka terdiri daripada pembekal, pakar runding, agensi kerajaan dan sebagainya. |
| Pengguna | Staf dan pelajar yang menerima dan mendapat perkhidmatan daripada UiTM. |
| *Service Level Agreement* (SLA) | Satu penyataan tahap perkhidmatan minimum yang perlu disediakan dan dipersetujui oleh UiTM dan Pembekal dalam kontrak perolehan bagi memastikan kelancaran projek yang dilaksanakan. |

## 2. PENYATAAN

### 2.1 PERKHIDMATAN RANGKAIAN UiTM

Merangkumi semua perkhidmatan rangkaian termasuk rangkaian berwayar, rangkaian tanpa wayar (WiFi) , *Wide Area Network* (WAN), peralatan rangkaian, perisian rangkaian dan teknologi yang digunakan.

2.1.1 Penggunaan Perkhidmatan Rangkaian UiTM

i. Hanya staf dan pelajar yang dibenarkan untuk mengakses ke rangkaian UiTM.
ii. Pihak ketiga perlu membuat pendaftaran sebelum menggunakan rangkaian UiTM.
iii. Penggunaan kemudahan rangkaian UiTM adalah untuk tujuan yang berkaitan dengan urusan UiTM.
iv. Penyediaan kemudahan rangkaian UiTM bagi tujuan majlis/ program rasmi universiti hendaklah dimohon melalui Sistem Perkhidmatan *Information and Communication Technology* (ICT) UiTM.
v. Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti tidak terhad kepada stesen kerja, komputer peribadi atau peralatan *Bring Your Own Device* (BYOD) yang menggunakan rangkaian UiTM.

2.1.2 Penyalahgunaan Rangkaian UiTM

Penyalahgunaan rangkaian UiTM boleh dikenakan tindakan tatatertib, surcaj dan/ atau tuntutan sivil terhadap pengguna dan pihak ketiga. Pengurusan ICT berhak menarik balik kemudahan penggunaan rangkaian UiTM jika didapati berlaku pelanggaran mana-mana peraturan yang ditetapkan seperti berikut:

i. Penggunaan kemudahan rangkaian UiTM untuk tujuan peribadi dan komersial bagi aktiviti yang bertentangan dengan undang-undang.
ii. Menggunakan rangkaian UiTM untuk aktiviti-aktiviti yang bertentangan dengan undang-undang termasuk menghantar, menerima dan menyebar maklumat yang berunsur ancaman, rahsia atau sulit mengenai UiTM.
iii. Memberi kemudahan rangkaian untuk digunakan oleh orang lain walaupun kepada pelajar atau staf UiTM tanpa mendapat kelulusan pentadbir rangkaian.
iv. Mengubah atau mengalih kedudukan peralatan rangkaian yang telah dipasang tanpa kebenaran.
*v.* Akses kepada aplikasi dan laman sesawang yang tidak dibenarkan atau dikategorikan sebagai *phishing, proxy, malware*, *adult-content, pornography, P2P dan gambling* dan perkara ini tertakluk kepada arahan semasa kerajaan.
vi. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen.
vii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.
viii. Penggunaan perisian/ peralatan pengintip (*sniffer*) atau penganalisis rangkaian (*network analyser*) tanpa kebenaran.
ix. Melaksanakan aktiviti *hacking, scanning, sniffing, phishing, encryption data* dan *crypto-mining* secara tidak sah di dalam atau ke luar universiti.
x. Penggunaan *Dynamic Host Configuration Protocol* (DHCP) *server* tanpa kebenaran Pengurusan ICT.
xi. Menukar *dynamic IP address* kepada *static IP address* tanpa kebenaran.
xii. Penggunaan *Domain Name Server* (DNS) selain dari DNS rasmi universiti adalah tidak dibenarkan.

2.1.3 Penyambungan ke Rangkaian UiTM

Setiap Pusat Tanggungjawab perlu memastikan peralatan ICT baharu dan peralatan yang menggunakan IP (IoT) yang akan disambungkan ke sistem rangkaian UiTM adalah IPV6 tersedia. Berikut adalah perkara yang perlu dipatuhi pengguna dan pentadbir rangkaian UiTM:

(a) Pengguna Rangkaian UiTM

i. Penyambungan peralatan ke rangkaian UiTM perlu mendapat kelulusan daripada Pengurusan ICT.
ii. Penggunaan rangkaian tanpa wayar (WiFi) UiTM perlu diaktifkan melalui portal – *wifi.uitm.edu.my*:
    a) *Wireless Access Point* - Semua jenis *wireless access point* yang bersambung ke rangkaian UiTM perlu mendapat kelulusan pemasangan daripada Pengurusan ICT.

b) *Service Set Identifier* (SSID) - SSID yang digunakan di seluruh UiTM ialah “UiTM WiFi STAF”, “UiTM WiFi STUDENT” , “UiTM WiFi GUEST”, “UiTM WiFi IoT Auth” dan “eduroam”.
c) PTj perlu mempunyai mekanisma kawalan akses yang bersesuaian bagi SSID “UiTM WiFi Guest”.
d) Pengurusan ICT UiTM tidak bertanggungjawab atas keselamatan penggunaan SSID selain dari yang dinyatakan di perkara (b).

iii. Pengurusan ICT berhak memutuskan penyambungan rangkaian yang dipasang tanpa kebenaran.
iv. Pengurusan ICT berhak menutup port yang menjejaskan keselamatan rangkaian UiTM.
v. Pengguna adalah bertanggungjawab memastikan peralatan yang disambungkan ke rangkaian UiTM adalah bebas dari *malicious code* seperti *spyware, adware, malware* dan *virus*.
vi. Pengguna adalah bertanggungjawab untuk memastikan setiap perisian adalah selamat digunakan.
vii. Peralatan yang menjadi sumber ancaman atau penyebar virus akan disekat capaiannya ke rangkaian UiTM.
viii. Sebarang penggunaan *static IP address* kepada peranti tertentu perlu dimohon kepada pihak pengurusan ICT.

(b) Pentadbir Rangkaian UiTM

i. Konfigurasi penyambungan yang dibuat oleh pembekal perlu di bawah pengawasan dan kawalan pentadbir rangkaian.
ii. Semua penggunaan domain perlu mendapat kelulusan Pengurusan ICT.
iii. Penggunaan alamat IP di bawah domain UiTM sama ada setempat atau global adalah mengikut peraturan yang ditetapkan oleh Pengurusan ICT.
iv. Penggunaan *port* yang dibuka dan servis yang berkaitan aplikasi adalah tanggungjawab pentadbir sistem.
v. Semua trafik dari dalam ke luar rangkaian UiTM dan sebaliknya mesti melalui *firewall*.
vi. Penentuan had akses perkakasan rangkaian dilaksanakan bagi memastikan kawalan capaian.

## 2.2 PERKHIDMATAN *VIRTUAL PRIVATE NETWORK* (VPN)

*Virtual Private Network* (VPN) ialah satu teknologi yang membolehkan sambungan selamat dan sulit ke rangkaian organisasi melalui rangkaian awam seperti Internet. VPN mengenkripsi komunikasi data dan memberikan akses seolah-olah pengguna berada di dalam rangkaian dalaman organisasi. VPN digunakan untuk:

i. Mengakses sistem dan aplikasi dalaman UiTM dari luar kampus dengan selamat.
ii. Menjalankan tugasan kritikal seperti pentadbiran sistem, pengemaskinian data, atau pemantauan sistam dan aplikasi kritikal universiti (contohnya sistem akademik).
iii. Menyokong kerja jarak jauh (remote working) dengan pematuhan kepada dasar / polisi keselamatan UiTM.
iv. Menyediakan saluran komunikasi yang terlindung semasa pemindahan maklumat sensitif.

2.2.1 Risiko Keselamatan Siber Dalam Penggunaan VPN

Pendedahan akaun VPN kepada pihak yang tidak sah boleh membawa kepada risiko keselamatan siber yang serius, antaranya:

i. Akses tidak sah kepada sistem dan aplikasi UiTM (terutama kepada sistem kritikal) yang boleh membawa kepada pengubahsuaian data, gangguan operasi atau kebocoran maklumat sulit.
ii. Pelanggaran data yang menjejaskan reputasi organisasi dan menyalahi peraturan akta seperti Akta Perlindungan Data Peribadi (PDPA).
iii. Wujud kompromi ke atas infrastruktur ICT, termasuk pemasangan "malware", "ransomware" atau "backdoor" yang boleh digunakan untuk serangan siber pada masa hadapan.
iv. Gangguan perkhidmatan organisasi, termasuk kerugian kewangan, gangguan perkhidmatan awam dan isu pematuhan kepada dasar keselamatan ICT Kerajaan.

2.2.2 Penggunaan VPN

Berikut adalah perkara yang perlu dipatuhi pengguna VPN UiTM:

(a) Kelayakan Memohon Akaun VPN UiTM.
Akaun VPN hanya akan diberikan kepada pengguna yang mempunyai keperluan khusus untuk mengakses sistem rangkaian dalaman (LAN) UiTM dari rangkaian luar, tertakluk kepada kelulusan daripada Bahagian Keselamatan ICT UiTM. Pemohon yang layak dipertimbangkan termasuklah:
   i. Staf ICT yang terlibat dalam penyelenggaraan sistem dan pelayan secara jarak jauh.
   ii. Staf yang memerlukan capaian kepada laporan atau dashboard operasi dari luar pejabat.
   iii. Staf yang memerlukan akses kepada sistem dan aplikasi dalaman universiti atas dasar keperluan mendesak untuk operasi jabatan dan perlu dilaksanakan dari luar kampus.

(b) Semua permohonan akaun VPN adalah melalui Sistem UNITS dan perlu diteliti dan disokong oleh Ketua Jabatan dari segi aspek keselamatan dan risiko yang berkaitan (Rujuk perkara 2.2.1).

(c) Kelulusan capaian rasmi dari luar rangkaian UiTM adalah daripada Bahagian Keselamatan ICT, manakala sambungan capaian disediakan oleh Bahagian Infrastruktur Digital dan hendaklah menggunakan perkhidmatan VPN yang disediakan oleh UiTM.

(d) Ketua PTj perlu bertanggungjawab untuk memaklumkan kepada Bahagian Infrastruktur Digital sekiranya tiada keperluan staf untuk mendapat akaun VPN. Ini bagi mengelakkan sebarang penyalahgunaan akaun VPN.

(e) Semua perkakasan yang digunakan untuk mencapai rangkaian UiTM melalui VPN mestilah dilengkapi perisian antivirus dan perisian pengoperasian yang dikemaskini.

(f) ID dan kata laluan yang diberikan mestilah dilindungi dan tidak dikongsikan dengan individu lain.

(g) Pengguna yang diberi kemudahan VPN bertanggungjawab untuk memastikan kemudahan ini tidak disalah guna.
(h) Tempoh penggunaan mengikut keperluan dan tidak melebihi dua (2) tahun pada satu-satu masa. Untuk penggunaan melebihi tempoh yang ditetapkan, pengguna perlu membuat permohonan baharu.
(i) Akaun VPN akan dinyah aktif apabila pengguna bertukar jabatan atau tamat perkhidmatan.
(j) Tatacara dan prosedur permohonan boleh dirujuk di laman sesawang Jabatan Digital.

## 2.3 PENYEDIAAN INFRASTRUKTUR RANGKAIAN BAHARU

(a) Keperluan infrastruktur rangkaian mesti ditentukan secara bersama oleh pengguna dan Pengurusan ICT bagi setiap lokasi baharu/ diubahsuai. Perkara ini merujuk kepada Pekeliling Naib Canselor Bil.28/2006 bertarikh 3 Oktober 2006: Pelaksanaan Projek yang Melibatkan Sistem Rangkaian.

(b) Pengkabelan untuk Rangkaian Data Setempat (*Local Area Network*) dalam lingkungan 100-meter perlu menggunakan *Factory Made UTP Cable Patch Cord, modular jack*, *faceplate, patch panel* dan lain-lain peralatan yang berkaitan dengan pemasangan kabel.

(c) Kabel Fiber Optik (*indoor/outdoor*) digunakan bagi sambungan rangkaian melebihi 100-meter dan juga sebagai backbone bagi bangunan yang bertingkat dengan jarak melebihi 100 meter atau sambungan ke blok-blok berasingan, lengkap menggunakan *fiber patch panel* dan *standard connector pigtail* dan lain-lain peralatan yang berkaitan dengan pemasangan kabel.

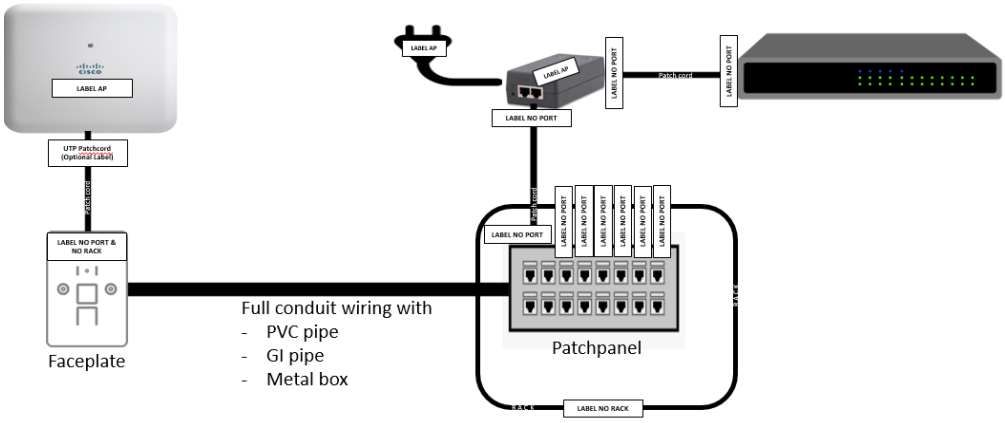
(d) Jarak 100-meter diukur bermula daripada peranti pengguna hingga *patch panel* di dalam rak Kerja-kerja pengkabelan fiber adalah menggunakan jenis seperti berikut:
   *i.* Dalam bangunan (*Indoor*): Penggunaan *fiber optik indoor multimode/singlemode.*
   *ii.* Luar bangunan (*Outdoor*): Penggunaan *fiber optik outdoor multimode/singlemode.*

(e) Kerja-kerja pengkabelan mesti menggunakan *cable trunking* yang bersesuaian seperti *paip Poly Vinyl Chloride* (PVC), *paip Galvanized Iron* (GI Pipe), *Metal Trunking* atau mana-mana yang bersesuaian dengan lokasi pemasangan. Pemasangan trunking juga perlu kemas dan sempurna bagi memastikan kekemasan pemasangan trunking di dinding atau siling.

(f) Kerja-kerja pengkabelan mesti menggunakan piawaian yang telah ditetapkan bagi kerja-kerja infrastruktur pendawaian seperti berikut:
   i. ANSI/TIA/EIA Cabling Standards;
   ii. ISO/IEC Cabling Standards;
   iii. AT&T/258A Standards; dan
   iv. Lain-lain yang berkaitan.

(g) Kerja-kerja pengkabelan dan material yang digunakan perlu mematuhi standard yang ditetapkan oleh *National Fire Protection Association, Local Electrical Code* dan *manufacturing standard* terkini.

(h) Semua kabel pendawaian perlu dilabel dan ditandakan mengikut ketetapan seperti berikut:




**Rajah 1: Pelabelan Peralatan Rangkaian**

(i) Dokumentasi kerja-kerja pengkabelan perlu disediakan untuk pengesahan kerja dan diserahkan dalam format *softcopy* dan *hardcopy* kepada UiTM selepas kerja-kerja pemasangan selesai. Dokumentasi ini perlu dikemaskini sekiranya terdapat perubahan pada pengkabelan asal.

(j) Tempoh jaminan kabel yang digunakan adalah sekurang-kurangnya dua puluh (20) tahun.

(k) Sebarang kesalahan dan ketidakpatuhan ke atas kerja-kerja pengkabelan ini akan mengakibatkan perkara seperti berikut:

i. Sambungan rangkaian yang melibatkan kerja-kerja pengkabelan yang salah perlu dibuka semula.

ii. Penahanan pembayaran sehingga kerja pengkabelan yang sempurna dilaksanakan.

## 2.4 KESELAMATAN PERALATAN RANGKAIAN

### 2.4.1 Keselamatan Fizikal

i. Peralatan rangkaian perlu ditempatkan di lokasi yang bebas daripada risiko di luar jangkaan seperti banjir, gegaran, kekotoran dan sebagainya.

ii. Peralatan rangkaian hanya boleh diakses oleh staf yang dibenarkan sahaja.

iii. Ruang penempatan peralatan rangkaian perlu mempunyai sistem pengudaraan yang baik.

iv. Memastikan peralatan rangkaian mendapat bekalan elektrik yang tidak terganggu.

v. Ruang penempatan peralatan rangkaian tidak boleh digunakan untuk tujuan lain tanpa kebenaran.

2.4.2 Capaian Fizikal

(a) Capaian Pengkabelan Rangkaian

i. Langkah-langkah sewajarnya perlu diambil untuk melindungi kabel rangkaian daripada digunakan oleh orang yang tidak berkenaan.
ii. Melindungi pengkabelan di dalam kawasan awam dengan cara memasang *conduit* atau lain-lain mekanisme perlindungan.
iii. Pusat pendawaian diletakkan di dalam ruang atau bilik yang berkunci dan hanya boleh diakses oleh staf yang dibenarkan sahaja.

(b) Capaian Peralatan Rangkaian

i. Peralatan perlu ditempatkan di lokasi yang selamat dan terkawal.
ii. Peralatan rangkaian hanya boleh diakses oleh staf yang dibenarkan sahaja.

2.4.3 Capaian Logikal

Akses kepada peralatan rangkaian iaitu *switch, access point, controller* dan *server* dihadkan kepada staf yang dibenarkan sahaja. Berikut adalah perkara yang perlu dipatuhi:

i. Semua akses kepada konfigurasi peralatan rangkaian dikawal melalui akaun yang disediakan oleh pentadbir rangkaian.
ii. Semua perubahan konfigurasi perisian dan perkakasan rangkaian perlu direkodkan termasuk nama pengguna yang membuat perubahan, pengesahan, tarikh dan masa.
iii. Perubahan konfigurasi perlu dikendalikan oleh pentadbir rangkaian.

2.4.4 Penyelenggaraan Perkakasan

i. Peralatan rangkaian perlu dipasang dan diselenggara mengikut *Service Level Agreement* (SLA) yang ditetapkan.
ii. Setiap kerja penyelenggaraan perlu direkodkan.

## 3. RUJUKAN

i. Dasar ICT UiTM.

ii. Polisi Keselamatan Siber UiTM

iii. Pekeliling Naib Canselor Bil.28/2006 bertarikh 3 Oktober 2006 - Pelaksanaan Projek yang Melibatkan Sistem Rangkaian