GARIS PANDUAN PENGGUNAAN BYOD *(Bring Your Own Device)*

UNIVERSITI KEBANGSAAN MALAYSIA

REKOD PINDAAN

Bil.	Tarikh Pindaan	Ringkasan	Kelulusan	Tarikh kuatkuasa
1.				
2.				

Kandungan	Muka surat

1.0 TUJUAN

Garis panduan ini menerangkan tentang tanggungjawab pemilik peralatan ICT peribadi (BYOD) yang digunakan untuk tugasan rasmi, mengendalikan maklumat rasmi dan rahsia rasmi Universiti termasuk mencapai Sistem Maklumat Universiti dalam persekitaran Universiti.

2.0 LATAR BELAKANG

Pihak Universiti telah membenarkan penggunaan BYOD bagi meningkatkan produktiviti dalam urusan pentadbiran serta menyokong aktiviti pembelajaran dan pengajaran. Namun begitu, penggunaan peralatan BYOD dalam persekitaran Universiti perlu dikawal selia bagi memastikan aset Universiti sentiasa terpelihara dan terkawal.

Bagi melaksanakan penggunaan BYOD, beberapa panduan dan kawalan keselamatan perlu dikuat kuasa oleh pihak Universiti dan dipatuhi oleh semua warga UKM.

3.0 SKOP

Garis panduan ini adalah terpakai untuk semua warga UKM yang menggunakan peralatan ICT milik peribadi di dalam kampus atau premis UKM.

Peralatan ICT milik peribadi merujuk kepada

a) Peralatan ICT yang bukan milik UKM; atau
b) Peralatan ICT yang diperolehi menggunakan kemudahan Elaun Komputer bagi kakitangan Akademik dan Pengurusan & Profesional (P&P) UKM.

4.0 DEFINISI DAN SINGKATAN

4.1 Definisi

BYOD	BYOD atau *bring your own device* merujuk kepada amalan warga UKM yang membawa peralatan ICT milik peribadi termasuk, tetapi tidak terhad kepada komputer riba, telefon pintar atau tablet ke dalam kampus dengan tujuan untuk melaksanakan tugasan rasmi, mencapai Sistem Maklumat Universiti, mengendalikan maklumat rasmi dan rahsia rasmi Universiti atau menggunakan rangkaian Universiti.

4.2 Singkatan

Peralatan BYOD	Peralatan ICT milik peribadi yang bertujuan untuk BYOD

5.0 TANGGUNGJAWAB PENGGUNA BYOD

Berikut adalah perkara yang perlu dipatuhi oleh semua pengguna peralatan BYOD di UKM:

5.1 Kawalan Kata laluan

a) Semua peralatan BYOD mestilah dilindungi dengan kawalan keselamatan (contoh: kata laluan atau kod pin).

b) Kata laluan yang digunakan untuk mencapai sistem dan maklumat Universiti mestilah mematuhi Garis Panduan Pengurusan Kata Laluan UKM dan dilindungi.

5.2 Perisian

a) Peralatan BYOD mestilah menggunakan perisian yang sah dan selamat sahaja.

b) Perisian berlesen Universiti tidak boleh dipasang atau dimuat turun ke peralatan BYOD kecuali dengan kebenaran pihak Universiti.

c) Pihak Universiti berhak menghalang peralatan BYOD yang telah diubah konfigurasi (contoh: *jailbreaking/rooted*) daripada mencapai sistem, maklumat atau rangkaian Universiti.

5.3 Capaian Rangkaian

a) Capaian ke internet atau intranet menggunakan rangkaian Universiti mestilah mematuhi Garis Panduan Penggunaan Rangkaian UKM yang ditetapkan.

b) Pihak Universiti berhak untuk menghalang capaian ke rangkaian Universiti jika peralatan BYOD tersebut tidak mematuhi garis panduan yang ditetapkan.

c) Bilangan peralatan yang dibenarkan untuk mencapai rangkaian Universiti bagi setiap pengguna adalah terhad kepada 3 unit peralatan.

5.4 Keselamatan Data

a) Semua maklumat rasmi dan rahsia rasmi Universiti adalah hakmilik UKM.

b) Pengendalian maklumat rasmi dan rahsia rasmi Universiti menggunakan peralatan BYOD perlulah mematuhi Garis Panduan Pengurusan Rahsia Rasmi Universiti/ Arahan Keselamatan/ peraturan yang berkuatkuasa.

c) Maklumat rasmi Universiti dan maklumat peribadi perlu diasingkan melalui pengurusan akaun/domain pengguna atau *folder* yang berbeza.

d) Semua maklumat rasmi dan rahsia rasmi Universiti perlu dihapus daripada peralatan BYOD sekiranya:

i. telah selesai atau tidak lagi menggunakannya
ii. mendapat arahan daripada pihak Universiti
iii. kakitangan berhenti atau bersara
iv. bertukar jabatan atau bidang tugas dan tidak lagi diberi capaian kepada maklumat tersebut.
v. peralatan akan dipindah milik
vi. peralatan diserahkan kepada pihak ketiga untuk dibaikpulih/diselenggara.

5.5 Perlindungan daripada malware

a) Peralatan BYOD yang digunakan mestilah mempunyai perlindungan daripada *malware*/virus seperti memasang perisian antivirus.

b) Pemilik peralatan BYOD perlu memastikan semua perisian yang dipasang pada peralatan BYOD adalah yang sah dan sentiasa dikemaskini termasuk *security updates* bagi menghalang ancaman atau serangan malware.

5.6 Perlindungan fizikal

a) Peralatan BYOD perlu dipelihara dan disimpan dengan baik dan selamat.

b) Peralatan yang hilang atau dicuri hendaklah dilaporkan segera kepada pihak Universiti untuk tindakan lanjut. (peralatan yang digunakan untuk tugasan rasmi atau mengandungi maklumat rasmi Universiti sahaja)

6.0 PEMANTAUAN DAN KAWALAN KESELAMATAN

6.1 Pihak Universiti bertanggungjawab untuk memastikan pelaksanaan BYOD adalah terkawal dan selamat. Oleh itu, pihak Universiti:

a) berhak untuk memantau peralatan BYOD yang digunakan dalam rangkaian UKM dan merekod log trafik capaian ke mana-mana peralatan dan sistem dalam UKM atau keluar masuk internet.

b) boleh menghalang peralatan BYOD untuk mencapai mana-mana sistem atau kemudahan rangkaian seperti WiFi jika peralatan tersebut didapati memberi ancaman keselamatan atau telah dikompromi oleh penggodam.

6.2 Pemilik peralatan BYOD hendaklah membenarkan pihak Universiti memasang perisian keselamatan dan menetapkan kawalan tertentu pada peralatan BYOD dengan tujuan untuk memastikan maklumat Universiti yang dimuat turun dan dikendalikan sentiasa terpelihara.

7.0 PEMATUHAN

Warga UKM yang tidak mematuhi garis panduan ini boleh mengakibatkan kemudahan penggunaan BYOD ditarik semula atau dihalang/digantung serta tindakan tatatertib boleh dikenakan terhadap mereka.