UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

GARIS PANDUAN

Keselamatan Kata laluan Pengguna ICT

UNIVERSITI KEBANGSAAN MALAYSIA

REKOD PINDAAN

Bil.	Tarikh Pindaan	Ringkasan	Kelulusan	Tarikh kuatkuasa
1.	21 NOV 2019	DOKUMEN BARU VERSI 1.0	MPTPTM PTM	21 NOV 2019
2.	12 JAN 2022	Pindaan dokumen perkara 4.3 (b)	MPTPTM PTM	12 JAN 2022
3.	19 OGO 2022	Pindaan perkara 4.2 (d) tambah perkataan ‘peribadi’	MPTPTM	19 OGO 2022

Kandungan	Muka surat

1.0 TUJUAN

Garis panduan ini menerangkan tatacara penguruusan kata laluan yang selamat.

2.0 LATARBELAKANG

Kata laluan adalah aspek penting dalam keselamatan ICT. Penggunaan kata laluan bertujuan untuk melindungi akaun pengguna dan memastikan maklumat universiti terpelihara daripada capaian yang tidak sah. Kelemahan pengurusan keselamatan kata laluan boleh mendedahkan sistem dan rangkaian universiti kepada serangan penggodam.

3.0 SKOP

Garis panduan ini merangkumi pengurusan keselamatan kata laluan pengguna ICT UKM.

4.0 KESELAMATAN KATA LALUAN

Berikut adalah perkara yang perlu dipatuhi bagi memastikan keselamatan kata laluan anda terjamin:

4.1 Memilih Kata laluan Yang Kukuh

a) Panjang kata laluan yang dipilih mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor atau simbol.
   - contoh kata laluan yang kukuh: p@55w0rd5@yA
   - contoh kata laluan yang lemah: abc123, 123456, password

b) Kata laluan mestilah tidak berdasarkan maklumat yang mudah diteka oleh orang lain seperti tarikh lahir atau nombor UKMPer.

c) Pastikan kata laluan yang berbeza digunakan untuk sistem yang berbeza. Contohnya, tidak menggunakan kata laluan yang sama untuk akaun emel dan perbankan internet.

4.2 Melindungi Kata laluan

Cara-cara melindungi kata laluan:

a) Kata laluan adalah hakmilik individu yang tidak boleh dikongsi dengan pihak lain.

b) Kata laluan adalah sulit dan tidak boleh didedahkan seperti ditampal pada monitor.

c) Sentiasa waspada kehadiran pihak lain semasa memasukkan kata laluan.

d) Tidak sesekali memberi kata laluan peribadi kepada pihak lain melalui e-mel, laman web atau media komunikasi lain.

e) Menggunakan fitur *remember password* adalah tidak dibenarkan pada peralatan atau komputer universiti.
f) Tidak menggunakan kata laluan *default*.

4.3 Menukar Kata laluan

Kata laluan perlu ditukar :

a) semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan diset semula.
b) sekurang-kurangnya satu (1) kali dalam tempoh satu (1) tahun.
c) sekiranya mengesyaki kata laluan telah disalahguna atau diketahui pihak lain.

5.0 PEMATUHAN

a) Semua pengguna ICT UKM bertanggungjawab untuk mengambil langkah yang sewajarnya seperti yang digariskan dalam dokumen ini.
b) Pentadbir sistem atau e-mel rasmi UKM berhak untuk mengeset semula kata laluan pengguna sekiranya didapati berlaku pencerobohan atau penyalahgunaan.
c) Sebarang penyalahgunaan kata laluan perlu dilaporkan kepada pentadbir sistem atau pentadbir emel UKM dan pihak UKMCERT.