HEBAHAN DIGITAL

OKTOBER
B/2026

MAKLUMAT PENGESAHAN DAN PENGURUSAN KATA LALUAN

Kata laluan hendaklah diuruskan secara selamat bagi mengurangkan risiko capaian tanpa kebenaran dan kompromi akaun pengguna. MBDK hendaklah mematuhi amalan terbaik pemilihan dan penggunaan kata laluan berdasarkan garis panduan yang ditetapkan seperi berikut :

A Kata laluan hendaklah diingat dan tidak boleh dikongsi, dicatat, disimpan atau didedahkan.

B Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan.

C Kata laluan hendaklah berlainan dengan pengenalan identiti pengguna dan tidak mudah diteka.

D Menggunakan kombinasi sekurang-kurangnya dua belas aksara dengan gabungan antara huruf, aksara khas dan nombor kecuali bagi sistem aplikasi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad.

E Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program.

F Sistem aplikasi hendaklah mempunyai tempoh masa aktif yang akan tamat selepas melebihi tempoh melahu (idle) yang ditetapkan seperti tidak melebihi 10 minit atau tertakluk kepada penetapan/kekangan sistem/aplikasi masing-masing.

G Sistem aplikasi yang dibangunkan hendaklah mempunyai kemudahan menukar kata laluan oleh pengguna.

H Penukaran kata laluan selepas log masuk kali pertama atau selepas penetapan semula kata laluan hendaklah dikuatkuasakan.

I Kemasukan atau cubaan kata laluan bagi capaian sistem aplikasi hendaklah mempunyai had maksimum. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula.

PERANAN

- *Pentadbir ICT,*
- *Pengguna,*
- *Pemilik Sistem*
- *Pegawai Keselamatan ICT (ICTSO).*

Sumber : Polisi Keselamatan Siber MBDK Versi 2.0
Grafik : Jabatan Teknologi Maklumat