1.0 TUJUAN

Garis panduan ini disediakan untuk membantu dalam proses tadbir urus dan kawalan akses serta interaksi individu terhadap sumber maklumat dan aset universiti .

2.0 SKOP

Merangkumi pengurusan terhadap pembentukan identiti pengguna, kaedah pengesahan identiti dan kawalan capaian serta interaksi individu kepada sistem maklumat dan aset universiti. Garis panduan ini terpakai kepada semua pelajar dan pekerja ~~staf~~ UPM serta pihak ketiga yang berurusan secara langsung yang menggunakan sistem maklumat dan perkakasan ICT UPM.

3.0 DOKUMEN RUJUKAN

Kod Dokumen	Tajuk Dokumen
-	Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi) 2014
-	Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)

4.0 PENGURUSAN IDENTITI

Pengurusan identiti merujuk kepada kaedah tadbir urus identiti individu di dalam sistem dan kawalan capaiannya terhadap sumber yang berada di dalam lingkungan sistem berkenaan berdasarkan hak penggunaan serta tahap capaian yang dibenarkan terhadap identiti tersebut.

4.1 PENGENALAN (*IDENTIFICATION*)

Pengenalan merupakan data yang menggambarkan seseorang individu atau sesebuah kumpulan. Pengenalan individu adalah menggunakan kata nama (ID pengguna ~~staf~~) yang didaftarkan.

i. Pendaftaran kata nama (ID pengguna) mestilah dibuat dengan arahan dan kebenaran pemilik proses / pemilik sistem.

ii. Kata nama (ID pengguna) bagi setiap pengguna mestilah unik dan dapat membuktikan serta mempunyai perkaitan dengan identiti individu berkenaan (contoh: nombor pekerja ~~staf~~ dan nama sebenar individu).

iii. Kata nama perlu mematuhi dan bersesuaian dengan batasan teknikal (*technical limitation*) sistem berkenaan seperti bilangan dan jenis aksara yang dibenarkan.

iv. Kata nama yang boleh menimbulkan kekeliruan sebagai contoh perkataan '*error*' dan '*password*', memecah belahkan (*disruptive*) dan bersifat menghina (*offensive*) perlu dielakkan.

v. Pengguna tidak dibenarkan sama sekali untuk mengakses ke sistem menggunakan ID pengguna selain ID sendiri.

~~vi. Penyelenggaraan maklumat kata nama pengguna perlu dibuat dengan kerap bagi mengelakkan berlakunya ID pengguna yang berulang.~~

vii. Penamatan atau penghapusan kata nama perlu dibuat dengan segera bagi pekerja ~~staf~~ yang tidak lagi berkhidmat dengan universiti

4.2 PENGESAHAN (*AUTHENTICATION*)

Mekanisme pengesahan dilaksanakan untuk membuktikan identiti individu melalui pilihan atau gabungan kaedah seperti berikut:-

- Kata laluan (*password*).
- Token atau kad pintar (*smart card*) .
- Biometrik
- Identiti Maya

UPM menggunakan kaedah kata laluan bagi pengesahan identiti individu atau pengguna untuk membolehkannya mencapai sistem maklumat atau perkakasan ICT yang berkaitan. Pengurusan kata laluan pengguna perlulah mengambil kira dan mematuhi ketetapan berikut:

i. Setiap pengguna diwajibkan untuk memilih kata laluan yang sukar untuk diteka atau diketahui oleh orang lain.

ii. Pengguna perlulah mencipta kata laluan:

(a) Panjang kata laluan sekurang-kurangnya 8 aksara dan dihadkan pada 40 aksara

(b) Sekurang-kurangnya 1 huruf kecil

(c) Sekurang-kurangnya 1 huruf besar

(d) Sekurang-kurangnya 1 angka (e) Tidak mengandungi ruang kosong / whitespace yang tidak kurang daripada lapan

(e) Penggunaan aksara khusus adalah digalakkan.

~~(8) aksara panjangnya dengan gabungan antara huruf dan nombor (alphanumerik).~~

iii. Jika terdapat kata laluan 'default', pertukaran kata laluan semasa *login* kali pertama dan/atau selepas *login* kali pertama atau selepas kata laluan diset semula perlu dikuatkuasakan.

iv. Pengguna juga digalakkan untuk mengubah kata laluan mereka dengan kadar kekerapan sekurang-kurangnya setiap tiga bulan supaya sukar untuk diteka secara rambang dan dimanipulasi.

~~v. Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum dua (2) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas tempoh masa selama 30 minit atau setelah diset semula oleh pegawai yang bertanggungjawab.~~

vi. Penggunaan '*built-in*' atau '*default user*' akaun bagi perkakasan komputer perlu dielakkan. Akaun ini perlu disekat dan akaun pengguna individu digunakan untuk mentadbir perkakasan berkenaan.

vii. Pembangun aplikasi perlu memastikan sistem yang dibangunkan hanya menyokong pengesahan (authentication) untuk kata laluan pengguna secara individu dan bukannya kumpulan (group).

viii. Aplikasi akan log keluar secara automatik sekiranyan tiada sebarang aktiviti atau tidak aktif selepas tempoh 15 minit (mengikut kesesuaian sistem).

4.3 KEIZINAN (*AUTHORIZATION*)

Keizinan (*Authorization*) adalah proses atau fungsi yang menyatakan hak capaian

seseorang individu kepada sumber atau aplikasi yang berkaitan dengannya. Kawalan akses ini boleh dibuat melalui kaedah berikut :

- *Role-based control.*
- *Task-based control.*
- Gabungan kaedah kawalan di atas.

Kaedah kawalan ini akan menentukan tahap capaian individu kepada sesuatu sistem atau aplikasi.

Pelaksanaan proses keizinan ini perlu mengambilkira perkara berikut:-

i. Capaian kepada data, aplikasi atau sistem perlu didefinisikan melalui polisi pengagihan tugas (*segregation of duties*), polisi keselamatan, keperluan pengguna atau peraturan organisasi.
ii. Klasifikasi pengguna perlu dibuat untuk untuk membezakan tanggungjawab di antara Pemilik Sistem / Pentadbir Proses, Pentadbir Sistem Pelaksana Operasi dan pengguna lain yang terlibat di dalam sesebuah sistem itu. Pengkelasan pengguna ini akan diterjemahkan dengah tahap capaian terhadap data dan sistem berkenaan.
iii. Pengkelasan pengguna perlu mengambil kira tahap akses kumpulan pengguna (*user group*). ~~yang meliputi kumpulan pentadbir proses, pentadbir sistem, pelaksana operasi dan juga pengguna biasa yang lain.~~
iv. Peranan dan peraturan / undang-undang perlu dipadankan dengan identiti pengguna bagi membolehkan kebenaran akses diberikan kepada pengguna tertentu.
v. Pemilik Sistem atau Pentadbir Proses bertanggungjawab menentukan individu yang dibenarkan untuk mengakses sesuatu sistem. Hak capaian perlu dibuat berdasarkan deskripsi dan bidang tugas pengguna sistem.
vi. Perubahan konfigurasi atau pelaksanaan operasi serta penyelenggaraan sistem oleh Pentadbir Sistem perlu dimaklumkan kepada ~~mendapat kebenaran~~ Pentadbir Proses sebelum dilaksanakan.
vii. Pemilik Sistem perlu mendokumenkan senarai pengguna sistem dan hak capaian mereka.

5.0 PENGURUSAN ID BERPUSAT

Pengurusan ID berpusat adalah perkhidmatan direktori pengenalan tunggal atau "*shared authentication database*" yang dibangunkan bagi mengatasi masalah berbilang id pengguna dan kata laluan. Semua sistem dan aplikasi UPM termasuk capaian ke rangkaian~~, emel~~ akan menggunakan satu identiti ~~ID pengguna dan katalaluan~~ yang sama.

Perkhidmatan operasi ID berpusat merangkumi aspek berikut:

~~i.~~ Pendaftaran dan pengeluaran ID pengguna ~~pelajar~~

a. Rekod ID pengguna ~~pekerja staf dan pelajar~~ baharu perlu diaktifkan secara automatik ke dalam sistem ID berpusat.

b. Penamatan dan penghapusan rekod ID pengguna ~~pekerja staf dan pelajar~~ perlu dilaksanakan dari sistem ID berpusat sekiranya telah tamat perkhidmatan/belajar atau tidak aktif.

ii. Pengaktifan dan penjagaan kata laluan

a. Pengaktifan dan penjagaan kata laluan dilaksanakan oleh pengguna sendiri tetapi dikawal selia oleh sistem ID berpusat.

iii. *Single Sign On* (SSO)

a. Membenarkan pengguna untuk log masuk ~~ke sistem hanya~~ dengan menggunakan satu set ID pengguna dan kata laluan bagi mengakses pelbagai aplikasi dan sistem.

b. Pengguna hanya perlu sekali log masuk bagi mengakses pelbagai aplikasi dan sistem.