1.0 SKOP

Prosedur ini digunapakai untuk memastikan tahap perlindungan setiap maklumat dan aset dilaksanakan seperti yang dipersetujui mengikut pengkelasan dan pengendalian aset ICT yang melibatkan aset dalam format fizikal dan elektronik.

2.0 TANGGUNGJAWAB

Wakil Pengurusan dan sesiapa yang terlibat adalah bertanggungjawab memastikan prosedur ini dilaksanakan.

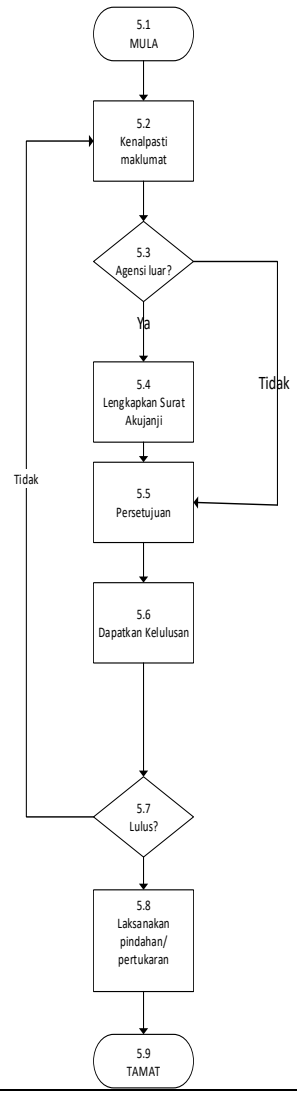
3.0 DOKUMEN RUJUKAN

Kod Dokumen	Tajuk Dokumen
MS ISO/IEC 27001:2013	*Information Technology – Security Techniques – Information Security Management Systems – Requirements*
-	Arahan Keselamatan Kerajaan Malaysia
-	Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi

4.0 TERMINOLOGI DAN SINGKATAN

Ketua Bahagian/Seksyen	:	Pekerja yang berhak untuk menyemak
KS	:	Ketua Seksyen yang bertugas di Seksyen iDEC yang dipertanggungjawabkan
PYB	:	Pekerja yang bertanggungjawab
Pekerja ICT	:	Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/ Juruteknik Komputer/Pekerja lain yang dilantik untuk mengurus ICT
Pentadbir Sistem	:	Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/ Juruteknik Komputer/Pekerja lain yang mengurus operasi atau aktiviti berkaitan pengoperasian aplikasi serta pengurusan sistem pangkalan data Universiti.
TPKD	:	Timbalan Pegawai Kawalan Dokumen
TWP	:	Timbalan Wakil Pengurusan
WP	:	Wakil Pengurusan
Pembekal	:	Pihak luar (organisasi atau individu) yang menyediakan produk, perkhidmatan, atau sumber tertentu kepada organisasi.

5.0 PROSES TERPERINCI

Tanggung jawab	Carta Alir	Perician	Rekod/ Dokumen Rujukan
Pekerja ICT Pembekal Pekerja ICT Pekerja ICT Pekerja ICT		5.2 Kenal pasti setiap maklumat atau perisian yang akan dilakukan pertukaran mengikut kesesuaian maklumat tersebut. Klasifikasi maklumat perlu di kenal pasti berdasarkan klasifikasi maklumat dalam Arahan Keselamatan Kerajaan Malaysia. 5.3 (a) Sekiranya agensi dalaman(UPM), terus ke langkah 5.5 (b) Sekiranya agensi luar, terus ke langkah seterusnya. 5.4 Lengkapkan Surat Aku janji beserta maklumat yang diperlukan. 5.5 Dapatkan persetujuan dari pihak penerima berkenaan maklumat atau perisian yang akan dihantar. 5.6 (a) Dapatkan kelulusan dari kedua-dua pihak iaitu penghantar dan penerima maklumat atau perisian tersebut. (b) Pastikan Ketua menyemak dan beri pertimbangan sewajarnya terhadap pertukaran maklumat tersebut. 5.7 (a) Sekiranya Ya, ikut langkah 5.7 (b) Sekiranya Tidak, kembali ke langkah 5.2 5.8 Tindakan susulan yang perlu diambil haruslah ditentukan.	

6. REKOD

Bil	Kod Fail, Tajuk Fail dan Senarai Rekod	Tanggungjawab Mengumpul dan Memfail	Tanggungjawab Menyelenggara	Tempat dan Tempoh Simpanan	Kuasa Melupus
1	Perpindahan atau Pertukaran Maklumat	Pekerja ICT	Penyelia PTJ	Rak Fail 3 Tahun	Ketua Pengarah Arkib Negara Malaysia

1.0 TUJUAN

Garis panduan ini disediakan untuk rujukan pekerja Universiti Putra Malaysia dalam melaksanakan enkripsi fail bagi memastikan kerahsiaan data sentiasa terpelihara dalam komunikasi data, dan meningkatkan keyakinan pengguna terhadap tahap keselamatan sistem aplikasi yang digunakan.

Enkripsi fail adalah proses mengubah suatu teks asli menjadi teks yang tersembunyi. Dalam kriptografi, enkripsi adalah proses di mana maklumat tidak dapat dibaca tanpa pengetahuan khusus.

2.0 PANDUAN

2.1 SKOP

(a) Semua sistem ICT yang mempunyai sambungan Rangkaian UPMNet.

(b) Semua Sistem Aplikasi Web UPM merangkumi:
   (i) Semua Sistem Aplikasi Web Baru yang dibangunkan secara dalaman atau *outsource*; dan

   (ii) Semua Sistem Aplikasi Web Baru yang dicapai secara Intranet sahaja atau kedua-duanya sekali.

2.2 RASIONAL MENGGUNAKAN ENKRIPSI

(a) Data dalam fail elektronik tanpa perlindungan keselamatan ICT boleh mengakibatkan pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin.

(b) Enkripsi adalah satu kaedah bagi memelihara data, di mana data asal (*plain text*) akan ditukar ke dalam bentuk data yang sukar difahami (*ciphertext*) dengan menggunakan algoritma enkripsi. Kata laluan adalah perlu bagi membuka dan membaca fail yang telah di enkrip.

(c) Kata laluan harus dimaklumkan secara berasingan kepada penerima fail yang di enkrip.

2.3 ENKRIPSI DALAM PENGHANTARAN DATA

(a) Enkripsi SSL/TLS perlu dilakukan terhadap protocol HTTP(s) bagi sistem aplikasi yang mempunyai data sensitif.
(b) Enkripsi perlu dilakukan terhadap data sensitif yang dikomunikasikan melalui media luaran dan email.
(c) Penggunaan VPN diwajibkan bagi akses pentadbiran (*admin access*) pelayan di pusat data.

2.4 ENKRIPSI DALAM PENGURUSAN INFRASTRUKTUR [TBC]

(a) Enkripsi perlu dilakukan terhadap data sensitif dalam pelayan.
(b) Enkripsi perlu dilakukan terhadap data sensitif dalam proses backup.

1.0 TUJUAN

Garis panduan ini disediakan untuk rujukan Pekerja Universiti Putra Malaysia yang mempunyai akses kepada rangkaian UPMNet, data dan sistem dalam melaksanakan kaedah-kaedah yang selamat bagi penggunaan peralatan mudah alih demi untuk melindungi pengguna, peralatan mudah alih, kerahsiaan data sensitif, integriti data dan aplikasi, dan ketersediaan perkhidmatan di Universiti Putra Malaysia.

2.0 PANDUAN

BIL	TINDAKAN	TANGGUNGJAWAB
1.	**KEPERLUAN PENGGUNA** i. Peralatan mudah alih yang telah *Jailbreak* dan *rooted* tidak dibenarkan. ii. Peralatan mudah alih mesti dilindungi oleh kata laluan kunci skrin dengan konfigurasi *timeout* dan *lock out*. iii. Peralatan mudah alih hendaklah sentiasa dikemaskini dengan sistem pengoperasian dan *patch* terkini. iv. Data dan maklumat korporat di dalam peralatan mudah alih perlu ~~dienkripsi~~ dikunci (dienkripsi). v. Pengguna tidak boleh memuatkan perisian cetak rompak atau kandungan yang tidak dibenarkan ke dalam peralatan mudah alih. vi. Aplikasi yang dimuat turun mesti melalui sumber yang dipercayai sahaja. vii. Peralatan mudah alih mesti mempunyai perisian antivirus. viii. Elakkan daripada menggunakan *public wifi* untuk akses data korporat. ix. Memiliki fungsi mengunci peranti dan menghapus data sekiranya berlaku kehilangan peralatan mudah alih. x. Perkongsian fail di atas awan (*cloud file sharing*) hanya boleh menggunakan penyedia yang dilanggan oleh universiti sahaja.	Pekerja Universiti Putra Malaysia

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

2.0 PANDUAN

2.1 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.

2.1.1 PENGENALAN (*IDENTIFICATION*)

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

BIL	TINDAKAN	TANGGUNGJAWAB
1	Pendaftaran kata nama (ID pengguna) mestilah dibuat dengan arahan dan kebenaran pemilik proses/pemilik sistem.	PYB
2	Kata nama (ID pengguna) bagi setiap pengguna mestilah unik dan dapat membuktikan serta mempunyai perkaitan dengan identiti individu berkenaan (contoh: ~~nombor pekerja~~ UPM-ID ~~dan nama sebenar individu~~).	PYB
3	Kata nama perlu mematuhi dan bersesuaian dengan batasan teknikal (*technical limitation*) sistem berkenaan seperti bilangan dan jenis aksara yang dibenarkan.	Pekerja dan Pelajar UPM

BIL	TINDAKAN	TANGGUNGJAWAB
4	Kata nama yang boleh menimbulkan kekeliruan sebagai contoh perkataan '*error*' dan '*password*', memecah belahkan (*disruptive*) dan bersifat menghina (*offensive*) perlu dielakkan.	Pekerja dan Pelajar UPM
5	Pengguna tidak dibenarkan sama sekali untuk mengakses ke sistem menggunakan ID pengguna selain ID sendiri.	Pekerja dan Pelajar UPM
6	Penamatan atau penghapusan kata nama perlu dibuat dengan segera bagi pengguna yang telah tamat perkhidmatan/belajar atau tidak aktif.	PYB

2.1.2 PENGESAHAN (*AUTHENTICATION*)

Mekanisma 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:

BIL	TINDAKAN	TANGGUNGJAWAB
1	Setiap pengguna diwajibkan untuk memilih kata laluan yang sukar untuk diteka atau diketahui oleh orang lain.	Pekerja dan Pelajar UPM
2	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	Pekerja dan Pelajar UPM

BIL	TINDAKAN	TANGGUNGJAWAB
	(d) Sekurang-kurangnya 1 angka (e) Tidak mengandungi ruang kosong/*whitespace* yang tidak kurang daripada lapan (f) Penggunaan aksara khusus adalah digalakkan	
3	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.	Pekerja dan Pelajar UPM
4	Pengguna juga digalakkan untuk mengubah kata laluan mereka dengan kadar kekerapan sekurang-kurangnya setiap tiga bulan supaya sukar untuk diteka secara rambang dan dimanipulasi.	Pekerja dan Pelajar UPM
5	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.	Pekerja dan Pelajar UPM
6	Pembangun aplikasi perlu memastikan sistem yang dibangunkan hanya menyokong pengesahan (*authentication*) untuk kata laluan pengguna secara individu dan bukannya kumpulan (*group*).	PYB
7	Aplikasi akan log keluar secara automatik sekiranya~~n~~ tiada sebarang aktiviti atau tidak aktif selepas tempoh 15 minit (mengikut kesesuaian sistem).	PYB

2.1.3 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 mengambil kira perkara berikut:-

BIL	TINDAKAN	TANGGUNGJAWAB
1	Capaian kepada data, aplikasi atau sistem perlu didefinisikan melalui polisi pengagihan tugas (*segregation of duties*), polisi keselamatan, keperluan pengguna atau peraturan organisasi.	PYB
2	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 dengan tahap capaian terhadap data dan sistem berkenaan.	PYB
3	Pengkelasan pengguna perlu mengambil kira tahap akses kumpulan pengguna (*user group*).	PYB
4	Peranan dan peraturan/undang-undang perlu dipadankan dengan identiti pengguna bagi membolehkan kebenaran akses diberikan kepada pengguna tertentu.	PYB
5	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.	PYB
6	Perubahan konfigurasi atau pelaksanaan operasi serta penyelenggaraan sistem oleh Pentadbir Sistem perlu dimaklumkan kepada Pentadbir Proses sebelum dilaksanakan.	PYB
7	Pemilik Sistem perlu mendokumenkan senarai pengguna sistem dan hak capaian mereka.	PYB

2.2 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 akan menggunakan satu identiti yang sama.

Perkhidmatan operasi ID berpusat merangkumi aspek berikut:

BIL	TINDAKAN	TANGGUNGJAWAB
1	Pendaftaran dan pengeluaran ID pengguna a. Rekod ID pengguna baharu perlu diaktifkan secara automatik ke dalam sistem ID berpusat. b. Penamatan dan penghapusan rekod ID pengguna perlu dilaksanakan dari sistem ID berpusat sekiranya telah tamat perkhidmatan/belajar atau tidak aktif.	PYB
2	Pengaktifan dan penjagaan kata laluan a. Pengaktifan dan penjagaan kata laluan dilaksanakan oleh pengguna sendiri tetapi dikawal selia oleh sistem ID berpusat.	PYB
3	*Single Sign On* (SSO) a. Membenarkan pengguna untuk log masuk 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.	PYB