1.0 TUJUAN

Garis panduan ini disediakan sebagai panduan untuk memastikan langkah-langkah pengendalian maklumat dilakukan mengikut langkah perlindungan yang telah ditetapkan bagi mengelakkan berlakunya penyalahgunaan atau kebocoran maklumat serta melindungi data dan maklumat dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan tanpa izin di Pusat Pembangunan Maklumat & Komunikasi, UPM (iDEC).

2.0 KLASIFIKASI MAKLUMAT

Dalam konteks keselamatan maklumat, Maklumat diklasifikasikan berdasarkan kepada sensitiviti suatu data dan kesannya kepada universiti sama ada data tersebut perlu didedahkan, diubahsuai atau dimusnahkan tanpa kebenaran. Pengklasifikasian data dapat membantu dalam melindungi maklumat berdasarkan kepada kawalan keselamatan yang bersesuaian. Maklumat diklasifikasikan kepada lima (5) peringkat sensitiviti :

Peringkat	Sensitiviti/Klasifikasi Maklumat
Rahsia Besar	Maklumat diklasifikasikan sebagai RAHSIA BESAR apabila dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada universiti.
Rahsia	Maklumat diklasifikasikan sebagai RAHSIA apabila dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan universiti menyebabkan kerosakan besar kepada kepentingan

Peringkat	Sensitiviti/Klasifikasi Maklumat
	dan martabat universiti atau memberi keuntungan besar kepada pihak luar.
Sulit	Maklumat diklasifikasikan sebagai SULIT apabila dokumen rasmi, maklumat rasmi dan bahan rasmi didedahkan, diubahsuai atau dimusnahkan tanpa kebenaran walaupun tidak membahayakan keselamatan universiti tetapi memudaratkan kepentingan atau martabat universiti atau orang perseorangan atau menjatuhkan imej universiti atau menguntungkan pihak luar.
Terhad	Maklumat diklasifikasikan sebagai TERHAD/DALAMAN apabila dokumen rasmi, maklumat rasmi dan bahan rasmi didedahkan, diubahsuai atau dimusnahkan tanpa kebenaran tetapi kawalan Keselamatan atau tahap perlindungan keselamatan yang bersesuaian perlu diberikan ke atas maklumat tersebut.
Terbuka	Maklumat diklasifikasikan sebagai TERBUKA apabila dokumen rasmi, maklumat rasmi dan bahan rasmi didedahkan, diubahsuai atau dimusnahkan dengan kebenaran untuk pengetahuan, tontonan atau kegunaan awam.

Jadual 1 : Klasifikasi Maklumat

3.0 KEPERLUAN PENGENDALIAN MAKLUMAT

Keperluan pengendalian maklumat dikenalpasti bagi melindungi maklumat dan penting untuk difahami bahawa sensitiviti suatu maklumat tidak hanya bergantung kepada kerahsiaan tetapi memerlukan integriti dan kebolehsediaan suatu maklumat tersebut.

3.1 KESELAMATAN DAN PERLINDUNGAN MAKLUMAT

Jadual 2 di bawah menerangkan keperluan perlindungan bagi melindungi maklumat berdasarkan kepada klasifikasi/sensitiviti yang telah ditetapkan.

Kategori Kawalan Keselamatan	Sensitiviti/Klasifikasi Maklumat		
	SULIT	**TERHAD**	**TERBUKA**
Kawalan Akses	i. Paparan dan pengubahsuaian terhad kepada individu yang diberi kuasa. ii. Pemilik data atau PYB diberi kebenaran untuk mengakses bersama kelulusan dari penyelia. iii. Keperluan Perjanjian Kerahsiaan	i. Paparan dan pengubahsuaian terhad kepada individu yang diberi kuasa. ii. Pemilik data atau PYB diberi kebenaran untuk mengakses bersama kelulusan dari penyelia.	i. Tiada sekatan untuk paparan umum. ii. Kebenaran oleh pemilik data diperlukan untuk pengubahsuaian
Cetakan/Salinan (Kertas dan elektronik)	i. Maklumat dicetak apabila terdapat keperluan yang sah ii. Salinan terhad kepada individu yang diberi kuasa untuk mengakses data.	i. Maklumat dicetak apabila terdapat keperluan yang sah ii. Salinan terhad kepada individu yang diberi kuasa untuk mengakses data.	i. Tiada halangan/ sekatan

Kategori Kawalan Keselamatan	Sensitiviti/Klasifikasi Maklumat		
	SULIT	**TERHAD**	**TERBUKA**
	iii. Maklumat tidak harus dibiarkan pada pencetak/faks. iv. Salinan mesti di label sebagai SULIT. v. Maklumat yang dihantar menggunakan sampul surat perlu ditandakan/dicop sebagai SULIT.	iii. Maklumat tidak harus dibiarkan pada pencetak/faks. iv. Maklumat dihantar menggunakan emel universiti.	
Keselamatan Rangkaian	i. Perlindungan menggunakan firewall yang disyorkan. ii. Menggunakan IDS dan IPS yang disyorkan. iii. *Server hosting* tidak terdedah ke seluruh rangkaian. iv. Firewall diselenggara secara berkala.	i. Perlindungan menggunakan firewall yang disyorkan. ii. Menggunakan IDS dan IPS yang disyorkan. iii. *Server hosting* tidak terdedah ke seluruh rangkaian internet	i. Perlindungan menggunakan firewall yang disyorkan. ii. Menggunakan IDS dan IPS yang disyorkan.
Keselamatan Sistem	i. Pengurusan dan keselamatan OS mengikut prosedur dan garis panduan ditetapkan.	i. Pengurusan dan keselamatan OS mengikut prosedur dan garis panduan ditetapkan. ii. IDS berdasarkan kepada hos	i. Pengurusan dan keselamatan OS mengikut amalan baik. ii. Hos berdasarkan kepada perisian

Kategori Kawalan Keselamatan	Sensitiviti/Klasifikasi Maklumat		
	SULIT	**TERHAD**	**TERBUKA**
	ii. IDS berdasarkan kepada hos perisian/IPS yang disyorkan.	perisian/IPS yang disyorkan.	firewall yang disyorkan.
Keselamatan Fizikal	i. Sistem mesti dikunci atau log keluar apabila tidak digunakan. ii. Keperluan keselamatan Pusat Data. iii. Pemantauan ke atas akses fizikal dan terhad kepada individu yang dibenarkan sahaja.	i. Sistem mesti dikunci atau log keluar apabila tidak digunakan. ii. Keperluan Keselamatan Pusat Data	i. Sistem mesti dikunci atau log keluar apabila tidak digunakan.
Remote Access	i. Terhad kepada rangkaian dalaman atau VPN universiti ii. *Remote Access* oleh pihak ketiga tidak dibenarkan tanpa penyeliaan.	i. Terhad kepada rangkaian dalaman atau VPN universiti ii. *Remote Access* oleh pihak ketiga terhad kepada akses sementara melalui prosedur yang telah diteapkan.	i. Tiada halangan/ sekatan
Storan Data	i. Keperluan storan di dalam persekitaran Pusat Data yang selamat. ii. Tidak boleh disimpan di ruang kerja individu	i. Keperluan storan di dalam persekitaran Pusat Data yang selamat. ii. Tidak boleh disimpan di ruang kerja	i. Keperluan storan di dalam persekitaran Pusat Data yang selamat.

Kategori Kawalan Keselamatan	Sensitiviti/Klasifikasi Maklumat		
	SULIT	**TERHAD**	**TERBUKA**
	(komputer/laptop persendirian) iii. Perlu menjalankan proses enkripsi terhadap media backup. iv. Jangan meninggalkan kertas/salinan keras maklumat di tempat terbuka. v. Simpan di lokasi yang selamat.	individu (komputer/laptop persendirian)	
Backup/Disaster Recovery	i. Keperluan backup harian. ii. Keperluan *off-site* storan di lokasi yang selamat.	i. Keperluan backup harian. ii. *off-site* storan yang disyorkan.	i. Keperluan backup harian.
Cakera Keras, CD, Tape, Kertas	i. Laporan pelupusan ii. Pelupusan/pemusnahan media elektronik.	i. Memadam rekod	i. Tiada halangan/ sekatan
Mobile Device	i. Menggunakan kawalan Kata laluan ii. Log keluar apabila tidak digunakan. iii. Laksanakan aktiviti enkripsi maklumat.	i. Menggunakan kawalan kata laluan. ii. Log keluar apabila tidak digunakan.	i. Menggunakan kawalan kata laluan yang disyorkan ii. Log keluar apabila tidak digunakan

Jadual 2 : Keselamatan dan Perlindungan Maklumat

3.2 PERLINDUNGAN MAKLUMAT ELEKTRONIK

Perlindungan maklumat digital atau elektronik memerlukan kaedah pengendalian maklumat yang berbeza seperti penggunaan enkripsi. Kaedah ini melibatkan aktiviti penukaran teks biasa (*plaintext*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses dekripsi digunakan.

Pengendalian Maklumat	Rahsia Besar	Rahsia	Sulit	Terhad	Terbuka
Penyimpanan					
Penyimpanan dalam media tetap/media boleh tukar	Enkripsi maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.				Tidak diperlukan
Menghantar / Memindahkan					
Menghantar maklumat melalui rangkaian awam	Menggunakan kaedah enkripsi				Tidak diperlukan

Jadual 3 : Pengendalian Maklumat Elektronik

3.2.1 PROSES ENKRIPSI

3.2.1.1 ENKRIPSI / DEKRIPSI

i. Salah satu kaedah yang praktikal untuk memelihara data adalah dengan menukarkannya ke dalam bentuk rahsia di mana penerima yang sah sahaja dapat memahaminya.

ii. Enkripsi (*Encryption*) - pengirim menukarkan mesej asal ke

bentuk rahsia dan menghantar kepada penerima.

iii. Dekripsi (*Decryption*) - menterbalikkan kembali proses enkripsi supaya mesej ditukar ke dalam bentuk yang asal.

3.2.1.2 ENKRIPSI / DEKRIPSI

i. Pengirim menggunakan algorithma enkripsi dan kunci untuk menukarkan data asal (*plaintext*) ke dalam bentuk data yang disulitkan (*cipher text*).

ii. Penerima menggunakan algorithma dekripsi dan kunci untuk menukarkan *cipher text* kembali ke data asal (*plaintext*).

iii. Kaedah enkripsi dan dekripsi boleh dibahagikan kepada 2 kategori :

a) Conventional (*secret key / symmetric*)

b) Public Key (*asymmetric*)