HURAIAN PINDAAN DOKUMEN ISO UPM

BAHAGIAN A: Huraian Pindaan Dokumen ISO

(Diisi oleh Pemohon/Pemilik Proses dan sila abaikan ruangan No. CPD kerana akan dilengkapkan oleh TPKD PP)

<table>
<tr><th rowspan="2">No. CPD</th><th rowspan="2">Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th rowspan="2">Tambahan (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th>Asal</th><th>Pindaan</th></tr>
<tr><td>ISMS SOK (IDEC): 1/2016</td><td>iDEC</td><td>Nama Dokumen: PROSEDUR PERTUKARAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/P002
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 01/06/2012</td><td>Nama Dokumen: PROSEDUR PERTUKARAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/P002
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/ PGR/MP</td><td>Manual Sistem Pengurusan Keselamatan Maklumat</td></tr><tr><td>MS ISO/IEC 27001:~~2007~~</td><td>Information Technology – Security Techniques – Information Security Management Systems –Requirements</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/ PGR/MP</td><td>Manual Sistem Pengurusan Keselamatan Maklumat</td></tr><tr><td>MS ISO/IEC 27001:2013</td><td>Information Technology – Security Techniques – Information Security Management Systems –Requirements</td></tr></table></td><td>P&T</td></tr>
<tr><td></td><td></td><td>4.0 TERMINOLOGI DAN SINGKATAN
PKD ISMS : Pegawai Kawalan Dokumen ISMS
Ketua Unit : Pegawai yang berhak untuk menyemak
PYB : Pegawai yang bertanggungjawab</td><td>5.0 TERMINOLOGI DAN SINGKATAN
PKD ISMS : Pegawai Kawalan Dokumen ISMS
Ketua Bahagian/ Seksyen/Unit : Pegawai yang berhak untuk menyemak
PYB : Pegawai yang bertanggungjawab</td><td>P&T</td></tr>
<tr><td></td><td></td><td>5.0 ~~TANGGUNGJAWAB~~</td><td>3.0 TANGGUNGJAWAB</td><td>P&T</td></tr>
<tr><td></td><td></td><td>6.0 ~~CARTA ALIR~~
Rujuk lampiran 1</td><td>6.0 PROSES TERPERINCI
Rujuk lampiran 1</td><td>P&T</td></tr>
<tr><td></td><td></td><td>~~8.0 REKOD ISMS~~</td><td>7.0 REKOD ISMS</td><td>P&T</td></tr>
<tr><td></td><td></td><td>~~9.0 SEJARAH SEMAKAN~~</td><td>8.0 SEJARAH SEMAKAN</td><td>P&T</td></tr>
</table>

<table>
<tr><th>No. CPD</th><th>Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th><u>Tambahan</u> (T) / <s>Pemotongan</s> (P)</th></tr>
<tr><th></th><th></th><th>Asal</th><th>Pindaan</th><th></th></tr>
<tr><td>ISMS SOK (IDEC): 1/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGENDALIAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 30/11/2012</td><td>Nama Dokumen: GARIS PANDUAN PENGENDALIAN MAKLUMAT
Kod Dokumen:UPM/ISMS/SOK/GP03/PENGENDALIAN MAKLUMAT
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr><tr><td>-</td><td><s>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</s></td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Arahan Keselamatan Kerajaan Malaysia</td></tr><tr><td>-</td><td><s>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</s></td></tr><tr><td><u>-</u></td><td><u>Panduan pengurusan Fail dan Rekod Universiti</u></td></tr></table></td><td>P&T</td></tr>
<tr><td>ISMS SOK (IDEC): 1/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN IDENTITI
Kod Dokumen:UPM/ISMS/SOK/GP07/IDENTITI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 05/06/2016</td><td>Nama Dokumen: GARIS PANDUAN PENGURUSAN IDENTITI
Kod Dokumen:UPM/ISMS/SOK/GP07/IDENTITI
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><s>Garis Panduan Teknologi Maklumat Komunikasi</s></td></tr></table></td><td>2.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><u>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</u></td></tr></table></td><td>P&T</td></tr>
<tr><td></td><td></td><td>4.2 PENGESAHAN (AUTHENTICATION)</td><td>4.2 PENGESAHAN (AUTHENTICATION)
<u>viii. Aplikasi akan log keluar secara automatik sekiranyan tiada sebarang aktiviti atau tidak aktif selepas tempoh 15 minit (mengikut kesesuaian sistem).</u></td><td>P&T</td></tr>
<tr><td></td><td></td><td></td><td><u>4.3 PENGURUSAN ID BERPUSAT</u>

<u>Pengurusan ID berpusat adalah perkhidmatan direktori pengenalan tunggal atau “shared authentication database” yang dibangunkan bagi mengatasi masalah berbilang id</u></td><td>T</td></tr>
</table>

<table>
<tr><th>No. CPD</th><th>Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th><u>Tambahan</u> (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th></th><th></th><th>Asal</th><th>Pindaan</th><th></th></tr>
<tr><td></td><td></td><td></td><td><u>pengguna dan kata laluan. Semua sistem dan aplikasi UPM termasuk capaian ke rangkaian, emel akan menggunakan satu ID pengguna dan katalaluan yang sama.</u>

<u>Perkhidmatan operasi ID berpusat merangkumi aspek berikut:</u>

i. <u>Pendaftaran dan pengeluaran pelajar</u>
a. <u>Rekod staf dan pelajar baharu perlu diaktifkan secara automatik ke dalam sistem ID berpusat.</u>
b. <u>Penamatan dan penghapusan rekod staf dan pelajar perlu dilaksanakan dari sistem ID berpusat sekiranya telah tamat perkhidmatan/belajar atau tidak aktif.</u>

ii. <u>Pengaktifan dan penjagaan kata laluan</u>
a. <u>Pengaktifan dan penjagaan kata laluan dilaksanakan oleh pengguna sendiri tetapi dikawal selia oleh sistem ID berpusat.</u>

iii. <u>Single Sign On (SSO)</u>
a. <u>Membenarkan pengguna untuk log masuk ke sistem hanya menggunakan satu set ID pengguna dan kata laluan.</u></td><td>T</td></tr>
<tr><td>ISMS SOK (IDEC): 2/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN ENKRIPSI FAIL
Kod Dokumen:UPM/ISMS/SOK/GP04/ENKRIPSI
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN ENKRIPSI FAIL
Kod Dokumen:UPM/ISMS/SOK/GP04/ENKRIPSI
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td>~~Garis Panduan Teknologi Maklumat Komunikasi~~</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><u>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</u></td></tr></table></td><td>P&T</td></tr>
</table>

<table>
<tr><th>No. CPD</th><th>Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th><u>Tambahan</u> (T) / <s>Pemotongan</s> (P)</th></tr>
<tr><th></th><th></th><th>Asal</th><th>Pindaan</th><th></th></tr>
<tr><td>ISMS SOK (IDEC): 2/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN KESELAMATAN PERALATAN MUDAH ALIH
Kod Dokumen:UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 24/10/2014</td><td>Nama Dokumen: GARIS PANDUAN KESELAMATAN PERALATAN MUDAH ALIH
Kod Dokumen:UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><s>Garis Panduan Teknologi Maklumat Komunikasi</s></td></tr></table></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>-</td><td>Kaedah-kaedah UPM (Teknologi Maklumat dan Komunikasi)</td></tr><tr><td>-</td><td><u>Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)</u></td></tr></table></td><td>P&T</td></tr>
<tr><td>ISMS SOK (IDEC): 2/2016</td><td>iDEC</td><td>Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT
Kod Dokumen:UPM/ISMS/SOK/P001
No. Isu:_01_, No. Semakan:_00_, Tarikh Kuatkuasa: 30/11/2012</td><td>Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT
Kod Dokumen:UPM/ISMS/SOK/P001
No. Isu:_01_, No. Semakan:_01_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>3.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/OPR/<s>KES</s>/ P004</td><td>Prosedur Pengendalian Insiden</td></tr><tr><td>Bilangan 4 Tahun 2006</td><td>Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.</td></tr><tr><td>Bilangan 1 Tahun 2001</td><td>Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi</td></tr></table></td><td>4.0 DOKUMEN RUJUKAN<table><tr><th>Kod Dokumen</th><th>Tajuk Dokumen</th></tr><tr><td>UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN</td><td>Garis Panduan Pengendalian Insiden</td></tr><tr><td>DRP-ICT UPM (3.0)</td><td>PELAN PEMULIHAN BENCANA ICT UPM</td></tr><tr><td>Bilangan 4 Tahun 2006</td><td>Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.</td></tr><tr><td>Bilangan 1 Tahun 2001</td><td>Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi</td></tr></table></td><td>P&T</td></tr>
</table>

<table>
<tr><th>No. CPD</th><th>Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th><u>Tambahan</u> (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th></th><th></th><th>Asal</th><th>Pindaan</th><th></th></tr>
<tr><td></td><td></td><td>6.0 PELAN TINDAK BALAS INSIDEN KESELAMATAN ICT
<table>
<tr><th>Proses</th><th>Aktiviti</th><th>Masa</th><th>Tindakan</th></tr>
<tr><td>Pembaikan</td><td>c. Tindakan pemulihan ke atas bencana berkaitan ICT hendaklah merujuk kepada manual:
~~- DRP Data Center~~
~~- DRP Sistem Sumber Manusia~~
~~- DRP Sistem Kewangan~~
~~- DRP Laman Web~~
~~- DRP Sistem Maklumat Pelajar~~</td><td>Mengikut masa yang ditetapkan</td><td>Pentadbir Sistem

Pentadbir Sistem

Pengarah iDEC</td></tr>
<tr><td>Pemantauan</td><td>d. Menyediakan laporan insiden dan makluman kepada ~~Pengurusan Universiti~~</td><td></td><td></td></tr>
</table></td><td>6.0 PELAN TINDAK BALAS INSIDEN KESELAMATAN ICT
<table>
<tr><th>Proses</th><th>Aktiviti</th><th>Masa</th><th>Tindakan</th></tr>
<tr><td>Pembaikan</td><td>c. Tindakan pemulihan ke atas bencana berkaitan ICT hendaklah merujuk kepada manual:
- <u>Pelan Pemulihan Bencana ICT UPM</u></td><td>Mengikut masa yang ditetapkan</td><td>Pentadbir Sistem

Pentadbir Sistem

Pengarah iDEC</td></tr>
<tr><td>Pemantauan</td><td>d. Menyediakan laporan insiden dan makluman kepada <u>Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi UPM</u></td><td></td><td></td></tr>
</table></td><td>P&T</td></tr>
<tr><td></td><td></td><td>7.0 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT
Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Rujuk ~~Prosedur Pengendalian Insiden (UPM/ISMS/OPR/KES/P004).~~</td><td>7.0 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT
Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Rujuk <u>Garis Panduan Pengendalian Insiden (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN).</u></td><td>P&T</td></tr>
<tr><td>ISMS SOK (IDEC): 2/2016</td><td>iDEC</td><td>Nama Dokumen: GARIS PANDUAN PENILAIAN RISIKO ASET
Kod Dokumen:UPM/ISMS/SOK/GP02/RISK ASSESSMENT
No. Isu:_01_, No. Semakan:_04_, Tarikh Kuatkuasa: 05/06/2015</td><td>Nama Dokumen: GARIS PANDUAN PENILAIAN RISIKO ASET
Kod Dokumen:UPM/ISMS/SOK/GP02/RISK ASSESSMENT
No. Isu:_01_, No. Semakan:_05_, Tarikh Kuatkuasa: 01/07/2016</td><td></td></tr>
<tr><td></td><td></td><td>1.TUJUAN
Garis panduan ini disediakan untuk menilai tahap risiko ~~aset ICT~~ supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan pelindungan dan kawalan ke atas aset ICT UPM.</td><td>1. TUJUAN
Garis panduan ini disediakan untuk menilai tahap risiko <u>keselamatan maklumat</u> supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas keselamatan maklumat UPM.</td><td>P&T</td></tr>
</table>

<table>
<tr><th>No. CPD</th><th>Pemilik Proses</th><th colspan="2">Huraian Pindaan Dokumen *</th><th>Tambahan (T) / ~~Pemotongan~~ (P)</th></tr>
<tr><th></th><th></th><th>Asal</th><th>Pindaan</th><th></th></tr>
<tr><td></td><td></td><td>

2. DEFINISI

Bil.	Terma	Deskripsi
1	Aset	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia. ~~Sila rujuk seksyen 8, Deskripsi langkah-langkah penilaian risiko: Pengenalpastian Aset (StepS3) untuk maklumat lanjut.~~
2	*Aset Yang bersandar*	Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi. ~~Sila rujuk seksyen 8, Deskripsi langkah-langkah penilaian risiko: Penilaian asset-aset dan penentuan kebergantungan antara asset-aset (Step S4)) untuk maklumat lanjut.~~
3	~~Pentadbir Proses (Owner)~~	Pentadbir Proses ~~juga sebagai pemilik risiko yang ebrtanggung terhadap risiko untuk sesuatu asset atau proses.~~
4	~~Pentadbir Sistem (Custodian)~~	Kakitangan Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset.
5	Risiko	Secara umum ..... kurang penjagaan yang sesuai.
6	Penilaian Risiko	Penilaian .... mudarat atau kerugian/kehilangan aset
7	*Ancaman*	~~Mengenalpasti potensi~~ sebarang kejadian atau perbuatan yang boleh menyebabkan satu atau lebih daripada perkara berikut berlaku: ..... Sesuatu ancaman boleh berlaku dengan semulajadi, sengaja atau tidak sengaja.

</td><td>

2. DEFINISI

Bil.	Terma	Deskripsi
1	Aset	Sesuatu yang bernilai yang boleh menyebabkan kerugian sekiranya hilang atau berubah. Berdasarkan MyRAM aset-aset tergolong kepada data/maklumat, perkhidmatan, perisian, perkakasan dan manusia.
2	*Aset Yang bersandar*	Subjek yang dinyatakan ketika kejadian sesuatu peristiwa. Bermakna aset lain diperlukan untuknya berfungsi
3	Owner/Pentadbir Proses **/Pemilik Risiko**	Pentadbir Proses yang bertanggungjawab **terhadap risiko** untuk sesuatu aset atau proses.
4	Custodian/ Pentadbir Sistem	Kakitangan Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset.
5	Risiko	Secara umum .... kurang penjagaan yang sesuai.
6	Penilaian Risiko	Penilaian ... mudarat atau kerugian/kehilangan aset
7	*Ancaman*	sebarang kejadian atau perbuatan yang boleh menyebabkan satu atau lebih daripada perkara berikut berlaku: ..... Sesuatu ancaman boleh berlaku dengan semula jadi, sengaja atau tidak sengaja.

</td><td>**P&T**</td></tr>
</table>

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	**Pindaan**	
		5.0 METODOLOGI PENILAIAN RISIKO ASET ICT ~~Semua agensi Kerajaan tertakluk untuk melaksanakan penilaian risiko aset ICT berasaskan metodologi Penilaian Risiko Terperinci MyRAM (*Malaysian Public Sector ICT Risk Assessment Methodology*) berpandukan kepada Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.~~ ~~Sepuluh (11) langkah utama dalam MyRAM adalah seperti berikut:~~ ~~1. Menubuhkan pasukan penilaian risiko~~ ~~2. Menetapkan sempadan aset~~ ~~3. Mengenal pasti Aset~~ ~~4. Mengenal pasti Pentadbir Proses dan Pentadbir Sistem;~~ ~~5. Menilai Aset~~ ~~6. Menilai Ancaman~~ ~~7. Menilai Kelemahan~~ ~~8. Mengenal pasti Kawalan~~ ~~9. Menganalisa Impak~~ ~~10. Menganalisa Kemungkinan~~ ~~11. Pengiraan Risiko~~ ~~Agensi hendaklah melaksanakan penilaian risiko berasaskan 10 langkah utama seperti di atas. Setiap langkah MyRAM saling bergantungan dengan menghasilkan satu atau lebih dokumen yang merupakan input kepada satu atau lebih langkah utama MyRAM.~~ ~~Sebarang pengemaskinian terhadap maklumat aset di dalam sistem MyRAM dilaksanakan apabila berlaku perubahan atau penambahan aset di dalam skop ISMS yang terlibat.~~	**5.0 METODOLOGI PENILAIAN RISIKO ASET ICT** Penilaian risiko ialah satu kaedah untuk menentukan apakah ancaman-ancaman yang wujud untuk sesuatu aset dan tahap risiko yang berkaitan dengan ancaman tersebut. Penentuan tahap risiko menyediakan organisasi dengan maklumat yang diperlukan untuk memilih perlindungan-perlindungan dan langkah kawalan yang bersesuaian untuk mengurangkan risiko kepada satu tahap yang boleh diterima. MAMPU telah membangunkan Malaysian Public Sector Information Security Risk Assessment Methodology atau MyRAM bagi membantu organisasi sektor awam dalam mengenalpasti dan menguruskan risiko keselamatan Maklumat. MAMPU akan menggunakan MyRAM untuk memastikan kesahihan maklumat dan aset Kerajaan dalam menyediakan perkhidmatan yang efektif dan efisien bagi semua pelanggan. Kami juga telah mengambil ISO/IEC 27005 sebagai contoh. **5.1 Kriteria Penilaian Risiko**: Kriteria bagi penilaian risiko UPM adalah seperti berikut: i. Semua risiko yang dinilaikan sebagai taraf "REND AH" akan dianggap Sebagai boleh diterima kepada pengurusan. ii. Risiko-risiko yang tidak menjejaskan Visi, Misi and Nilai-nilai UPM mungkin boleh dipertimbangkan untuk penerimaan. iii. Risiko-risiko yang tidak mempunyai impak ke atas reputasi, penjenamaan dan imej UPM mungkin boleh dipertimbangkan untuk penerimaan. iv. Risiko-risiko yang tidak mempunyai impak ke atas pematuhan perundangan mungkin boleh dipertimbangkan untuk penerimaan. v. Risiko-risiko yang mempunyai sedikit impak atau tiada kepada pengguna akhir, mungkin boleh dipertimbangkan untuk penerimaan.	**P&T**

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
		~~**6.0 CADANGAN PERINGKAT TINGGI**~~ ~~Keputusan bagaimana untuk mengendalikan risiko dan atribut yang perlu dipertimbangkan sebelum membuat keputusan dianalisis dan ditentukan. Cadangan peringkat tinggi akan dibentangkan oleh pasukan penilaian risiko kepada pihak pengurusan dalam laporan yang dijana oleh MYRAM.~~	**6.0 KEPERLUAN UNTUK PENILAIAN RISIKO** Penilaian risiko akan dilakukan untuk: i. Mengambilkira perubahan pada struktur organisasi dan aset baru; ii. Mempertimbangkan ancaman baru dan kelemahan; dan iii. Mengesahkan bahawa kawalan tetap efektif dan bersesuaian. iv. Mengesahkan risiko yang masih ada setelah kawalan untuk rawatan risiko dilaksanakan; v. Mengesahkan kriteria penilaian risiko oleh pihak pengurusan atasan.	**P&T**
		~~**7.0 KEPUTUSAN MENGENAI PILIHAN**~~ ~~Pada "Keputusan Pilihan", pasukan Risk Assessment akan mencadangkan kepada pihak pengurusan sama ada untuk menerima, mengurangkan, memindahkan, atau mengelakkan tahap risiko ancaman tertentu yang wujud di dalam aset tertentu. Penerangan bagi setiap pilihan keputusan adalah seperti berikut:~~	**7.0 PROSES PENILAIAN RISIKO** Pendekatan yang diambil adalah mengikut garis panduan proses penilaian risiko dalam dokumen MyRAM, bermula dari langkah Penubuhan Ahli Kumpulan sehingga Langkah 10, yang merupakan Pengiraan Risiko. Langkah-langkah ini berkaitan antara satu sama lain kerana input untuk satu aktiviti penilaian risiko boleh diambil daripada output langkah-langkah terdahulu. Jadual 1 dibawah, menunjukkan sepuluh (10) langkah latihan penilaian risiko.	**P&T**
		8.0	**8.0 PERANAN DAN TANGGUNGJAWAB AHLI KUMPULAN PENILAIAN RISIKO** i. Memberi nasihat kepakaran untuk aktiviti penilaian risiko ii. Mengurus aktiviti penilaian risiko iii. Memastikan selesai tepat pada masa; dan iv. Melakukan semakan semula untuk semua output dan dokumen sebelum dibentangkan kepada penasihat projek v. Sentiasa menentukan progres kerja; vi. Menilai keputusan-keputusan, jurang dan memberi maklum balas; dan vii. Melakukan semua tugasan yang disebut dalam langkah-langkah penilaian risiko	**T**

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
		9.0	**9.0 TARAF NILAI ASET** Berdasarkan Jadual 1 dibawah, kumpulan penilaian risiko perlu mewujudkan taraf nilai untuk keperluan Keselamatan Maklumat, iaitu Kerahsiaan/*Confidentiality* (C), Kesahihan/*Integrity* (I) dan Ketersediaan/*Availability* (A). Tahap-tahap *Low* (Rendah), *Medium* (Pertengahan)dan *High* (Tinggi) di Jadual 1 adalah berpandukan huraian yang diberi mengikut setiap skor. Dalam menilai sensitiviti setiap aset, Pasukan Penilaian Risiko akan menggunakan garis-garis panduan berikut: a) **Kerahsiaan (*Confidentiality*)** Kesan pendedahan maklumat rahsia/sulit yang tidak diluluskan boleh mengakibatkan kehilangan keyakinan pemegang saham dan mengaibkan. b) **Kesahihan (*Integrity*)** Kesan kepada sistem yang disebabkan dari pengubahsuaian aset secara sengaja, tanpa mendapat kelulusan atau tidak sengaja. c) **Ketersediaan (*Availability*)** Ini ialah kesan daripada penafian pengunaan aset secara sengaja atau kebetulan. Setiap aset mesti dinilai menurut tahap Confidentiality (Rahsia), Integrity (Kesahihan) dan Availability (Ketersediaan) masing-masing. **9.1 Kaedah Skor Untuk Risiko** Menggunakan Jadual 1 di bawah, selepas mengira nilai-nilai CIA dan nilai aset, sekarang kita perlu menghitung tahap risiko yang terdedah kepada aset-aset tersebut. Risiko-risiko wujud disebabkan kewujudan **Ancaman** kepada aset dan **Kelemahan** aset-aset itu sendiri 9.2 **Kebarangkalian & Impak** Dalam persekitaran sebenar, risiko yang dikenalpasti berdasarkan ancaman-ancaman dan kelemahan-kelemahan mungkin boleh berlaku atau tidak. Kemungkinan	**T**

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
			"peluang" risiko terjadi boleh bergantung kepada situasi. Oleh itu penilaian risiko adalah berdasarkan kepada "KebarangkalianTerjadi" dan "Impak" disebabkan sesuatu kejadian. Impak diukur kepada aset secara langsung, begitu juga impak kepada bisnes. Kebarangkalian dan Impak boleh dipilih berdasarkan Jadual 1 di bawah dan ditarafkan dari 3-1 berdasarkan huraian dalam Jadual.	
		10.0	**10.0 GARIS PANDUAN UNTUK KEPUTUSAN BAGI RISIKO YANG DIKENALPASTI** Output proses penilaian risiko adalah input bagi proses membuat keputusan yang menetapkan sama ada menerima, mengurangkan, memindahkan atau mengelakkan risiko yang sudah dikenalpasti. Ini akan dilakukan dalam Selection of Controls (Pemilihan Kawalan) dan ditunjukkan dalam Risk Treatment Plan (RTP) (Pelan Rawatan Risiko). Pasukan Penilaian Risiko akan menubuhkan High-Level-Recommendation untuk memperoleh kelulusan bertulis atau pengakuan daripada Jawatankuasa Kerja ISMS yang akan menentukan di dalam RTP apa yang mesti dilakukan selepas mendapat tahap risiko untuk semua aset-aset yang dikenalpasti. Di peringkat ini, keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan risiko yang telah kenalpasti mestilah dibuat hanya setelah latihan penilaian risiko selesai. Perlu mendapat pengesahan muktamad Timbalan Wakil Pengurusan ISMS. Secara asasnya membuat keputusan sama ada menerima, mengurangkan, memindahkan, atau mengelakkan tahap risiko adalah berdasarkan faktor-faktor masa, wang, tenaga kerja dan peralatan. Ketentuan pilihan untuk mengendali risiko boleh dilakukan dengan mengikuti langkah-langkah dalam Rajah 2 di bawah. Seperti yang digambarkan dalam Rajah 2 di atas, langkah pertama untuk membuat cadangan-cadangan High-Level ialah dengan mendapatkan keputusan tahap risiko-risiko dari Langkah 10. Kemudian tentukan apakah tahap risiko yang boleh diterima oleh Pasukan Penilaian Risiko. Rujuk Seksyen 4: Kriteria untuk menerima Risiko-risiko.	**T**

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
			Untuk Cadangan High-Level, terdapat dua (2) output iaitu: a) Keputusan atas pilihan; dan b) Strategi Perlindungan 10.1 **Keputusan atas Pilihan** Dalam Keputusan atas Pilihan, Kumpulan Penilaian Risiko akan mencadangkan kepada JawatanKuas Kerja ISMS sama ada untuk menerima, mengurangkan, memindahkan, atau mengelak tahap risiko ancaman yang wujud dalam sesuatu aset. Huraian-huraian untuk setiap pilihan keputusan ialah seperti berikut: a. **Menerima**: untuk menerima risiko-risiko berkaitan dengan aset-aset tanpa melaksanakan sebarang perlindungan atau kawalan b. **Mengurangkan**: melaksanakan kawalan untuk mengurangkan risiko. Mengurangkan tahap risiko adalah perlu apabila risiko tinggi. c. **Pemindahan**: Memindahkan risiko kepada entiti yang lain. d. **Mengelakkan**: untuk mengelak risiko-risiko apabila tiada pilihan lain. Pasukan Penilaian Risiko akan menerima, mengurangkan, memindahkan atau mengelakkan risiko bagi kriteria berikut: a. Memeriksa dan menilai sama ada risiko dapat diterima atau tidak. Kumpulan Penilaian Risiko boleh mencadangkan kepada pengurusan untuk menerima semua aset dengan tahap risiko Low (Rendah) dan tiada tindakan serta-merta diambil bagi melindungi aset; dan b. Jika risiko-risiko tidak boleh diterima, maka semak dan nilaikan sama ada ianya patut dikurangkan, dipindahkan atau dielakkan; c. Jika implikasi risiko-risiko membawa kepada bencana dan kritikal (High), risiko-risiko tersebut patut dikurangkan. Pengurangan Risiko akan dicapai melalui	

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
			pelaksanaan komponen-komponen berikut: operasi, prosedur, fizikal, Kakitangan dan keselamatan teknikal untuk memastikan bahawa operasi kritikal tidak terjejas. dan d. Jika implikasi risiko-risiko adalah sederhana kritikal (Medium), risiko-risiko tersebut boleh juga dipindahkan berdasarkan syarat-syarat berikut. i. Risiko-risiko mesti dipindahkan dengan adil. Risiko boleh dikongsi oleh pemilik-pemilik aset dan pihak ketiga. Misalnya, talian komunikasi bermasalah, dan Service Level Agreement (SLA) dengan penyedia talian menyatakan bahawa talian boleh didapati dalam 24 jam; bencana yang tidak dapat diketahui yang mungkin dialami pihak ketiga merupakan satu risiko yang dikongsi bersama dimana agensi bersediauntuk terima; dan ii. Risiko-risiko sepatutnya dielakkan sama sekali sekiranya tiada kawalan munasabah yang boleh dilaksanakan untuk mengurangkan risiko. Contoh, mengelak risiko-risiko ialah dengan memutuskan sistem. Pasukan Penilaian Risiko perlu membangunkan pelan perlindungan "*Risk Treatment Plan*" untuk dibentangkan kepada pengurusan. Bagi *Risk Treatment Plan,* kumpulan Penilaian Risiko perlu melihat samada kawalan yang sedia ada adalah cukup untuk melindungi aset-aset atau tidak. Jika kawalan yang sedia ada tidak mencukupi, kumpulan yang terbabit atau kumpulan pemilik risiko akan memilih objektif-objektif kawalan sesuai dan kawalan boleh didapati dalam *Annex A, ISO / IEC 27001:2005 ISMS Requirements*. Ini boleh didapati dalam *Statement of Applicability* atau Dokumen SOA.	**T**
		11.0	**11.0 KELULUSAN PENGURUSAN** a) Dokumen yang dibentangkan kepada Jawatankuasa Kerja ISMS untuk kelulusan maklumat analisis risiko mempunyai perkara-perkara berikut:	**T**

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	Pindaan	
			b) Sebarang syarat dan konsep-konsep yang baru atau berbeza – misalnya, aset-aset, ancaman-ancaman, risiko dan profil risiko - perlu dijelaskan. c) Maklumat ancaman, risiko dan kelemahan untuk setiap asset kritikal; d) Komposit, analisa keputusan-keputusan analisis risiko. Maklumat tersebut perlu dikemukakan dalam bentuk jadual atau grafik yang mudah dibaca. Implikasi mesti turut dijelaskan pada setiap tahap risiko yang sudah dikenal pasti; e) Amalan-amalan strategi perlindungan dan kelemahan-kelemahan organisasi dikumpulkan mengikut bidang amalan; dan f) Justifikasi untuk rancangan pelindungan g) Pengurusan tertinggi telah memutuskan bahawa semua risiko berbaki (risiko yang tinggal selepas menggunakan kawalan yang sesuai) hendaklah disifatkan sebagai 'Diterima' oleh pihak pengurusan.	T

BAHAGIAN B: Kelulusan CADANGAN PINDAAN DOKUMEN ISO

(Diisi oleh PKD / TPKD mengikut skop dokumen ISO)

Peneraju Proses:	PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI (iDEC)		
Kelulusan Mesyuarat:	Mesyuarat Jawatankuasa Kerja ISMS	**Kali ke-**	2
Tarikh Mesyuarat:	16 Jun 2016		
Cadangan Tarikh Kuatkuasa *:	1 Julai 2016		

Nota *:

- Tarikh Kuatkuasa merujuk kepada tarikh yang ditetapkan dan sila berhubung dengan PKD sekiranya perlukan tarikh kuarkuasa lain
- Masukkan Huraian Pindaan Dokumen yang dilampirkan oleh pencadang bersama Borang Cadangan Pindaan/Tambahan Dokumen.