DOKUMEN RUJUKAN
PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

http//www.upm.edu.my

DOKUMEN RUJUKAN PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT UPM

Senarai Kandungan

1. PENGENALAN

1.1 Pengenalan Sistem Pengurusan Keselamatan Maklumat (Information Security Management System – ISMS)

ISO/IEC 27001:2013 ISMS merupakan piawaian yang menetapkan satu set keperluan Sistem Pengurusan Keselamatan Maklumat. Istilah maklumat, merangkumi koleksi fakta dalam bentuk kertas atau mesej elektronik bagi mencapai misi dan objektif organisasi. Maklumat merangkumi sistem dokumentasi, prosedur operasi, rekod agensi, profil pelanggan, pangkalan data, fail data dan maklumat, maklumat arkib dan lain-lain.

Pembudayaan ISMS akan mewujudkan sistem penyampaian yang bukan sahaja memenuhi tuntutan serta kepuasan pengguna dan mematuhi peraturan semasa tetapi membolehkan sistem penyampaian beroperasi dalam keadaan baik, selamat dan terkawal.

ISMS turut menyediakan tanda aras (benchmark) tahap pengurusan keselamatan maklumat Universiti berasaskan piawaian antarabangsa serta memantapkan perlindungan maklumat dalam aset ICT berteraskan prinsip kerahsiaan, integriti dan ketersediaan.

ISMS dibangunkan berdasarkan kepada keperluan dalam Klausa 4: Konteks Organisasi hingga Klausa 10: Penambahbaikan dalam piawaian ISO/IEC 27001:2013 yang hendaklah dipatuhi mengikut keperluan piawaian.

1.2 Sejarah Pelaksanaan ISMS di UPM

UPM telah memulakan tindakan melaksanakan dengan adanya arahan daripada MAMPU yang telah meminta agar semua Universiti Awam dipersijilkan dengan ISO/IEC 27001 agar keselamatan maklumat terpelihara, diperoleh dengan cepat dan keselamatannya di kawal.

UPM telah mengorak langkah ke arah ISMS mulai 8 Disember 2011. Audit Peringkat Pertama telah diadakan pada 24 Oktober 2012, disusuli oleh Audit Peringkat Kedua pada 19 hingga 20 Disember 2012. Alhamdulillah UPM telah berjaya melepasi peringkat persijilan ini dengan memperolehi tujuh (7) peluang penambahbaikan. UPM telah berjaya memperolehi sijil ISMS bernombor AR5761 pada 4 Januari 2013.

Pada tahun 2018, menerusi Audit Pensijilan Semula SIRIM (kitaran kedua) yang diadakan pada 2 September & 1 - 3 Oktober 2018, UPM telah berjaya memperluaskan skop pensijilan ISMS kepada proses penilaian pengajaran prasiswazah di Fakulti bagi Kampus Serdang dan Bintulu. Sejajar dengan itu juga, no. Pensijilan ISMS telah dipinda kepada ISMS 00150 berdasarkan ketetapan terkini oleh pihak SIRIM.

2. PELAKSANAAN ISMS

2.1 Dasar ISMS

DASAR UNIVERSITI PUTRA MALAYSIA
(SISTEM PENGURUSAN KESELAMATAN MAKLUMAT) 2014

Universiti Putra Malaysia beriltizam mengadakan Sistem Pengurusan Keselamatan Maklumat yang berkesan melalui:

a) Pematuhan kepada kehendak organisasi dan perundangan serta peraturan;

b) Pembangunan objektif dan matlamat berdasarkan objektif keselamatan;

c) Komitmen bagi memenuhi keperluan berkaitan keselamatan maklumat; dan

d) Penilaian semula dan pengubahsuaian dasar, objektif dan sasaran untuk penambahbaikan berterusan.

PEMANSUHAN

Apa-apa dasar atau polisi mengenai pengurusan keselamatan maklumat Universiti Putra Malaysia yang berkuatkuasa sebelum ini adalah dimansuhkan.

ACADEMICIAN PROFESOR EMERITUS TAN SRI DATO'
DR. SYED JALALUDDIN SYED SALIM
Pengerusi Lembaga Pengarah
Universiti Putra Malaysia
9 Disember 2014

PERTANIAN • INOVASI • KEHIDUPAN

2.2 Skop Pensijilan, Pengecualian Skop dan Pusat Tanggungjawab (PTJ) yang Terlibat

Skop pensijilan ISMS UPM adalah:

i. Sistem Pengurusan Keselamatan Maklumat bagi Proses Pendaftaran Pelajar Baharu Prasiswazah Merangkumi Aktiviti Semakan Tawaran Hingga Pendaftaran Kolej Kediaman; dan

ii. Sistem Pengurusan Keselamatan Maklumat bagi Proses Penilaian Pengajaran Prasiswazah di Fakulti.

Pengecualian skop pensijilan ISMS proses pendaftaran pelajar baharu prasiswazah adalah kepada pendaftaran kursus, *Meal Plan* dan aktiviti kemasukan pendaftaran pelajar baharu prasiswazah untuk:

i. Pengajian Jarak Jauh;
ii. Program untuk Eksekutif; dan
iii. Antarabangsa.

PTJ terlibat adalah:

i. Pusat Jaminan Kualiti;
ii. Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik;
iii. Pusat Pembangunan Maklumat dan Komunikasi;
iv. Pejabat Penasihat Undang-Undang;
v. Pejabat Strategi Korporat dan Komunikasi ;
vi. Pejabat Pendaftar;
vii. Pejabat Bursar;
viii. Pusat Kesihatan Universiti;
ix. Bahagian Hal Ehwal Pelajar;
x. Bahagian Keselamatan Universiti;
xi. Perpustakaan Sultan Abdul Samad;
xii. Pejabat Pembangunan dan Pengurusan Aset;
xiii. Pusat Pembangunan Akademik;
xiv. Semua Kolej Kediaman;
xv. Semua Fakulti; dan
xvi. Universiti Putra Malaysia Kampus Bintulu, Sarawak.

2.3 Objektif ISMS

Objektif Keselamatan Maklumat yang telah dikenalpasti adalah seperti berikut:

BIL	PENYATAAN OBJEKTIF	PENERAJU
1.	Memastikan pelajar prasiswazah yang mengemukakan tawaran yang sah dibenarkan mendaftar	Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Kampus Serdang dan Bintulu)
2.	Memastikan pembayaran yuran pengajian adalah secara atas talian	Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Kampus Serdang dan Bintulu)
3.	Memastikan proses pemulihan sistem aplikasi pendaftaran pelajar baharu dapat dilaksanakan	Pasukan Pusat Data
4.	Memastikan *Service Level Agreement* (SLA) 95.0 sokongan ICT Pusat Data (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester	Pasukan Pusat Data
5.	Memastikan penilaian pengajaran setiap pelajar adalah rahsia	Pasukan Penilaian Pengajaran Prasiswazah di Fakulti
6.	Memastikan keyakinan pelajar terhadap keselamatan maklumat penilaian pengajaran berada pada tahap memuaskan	Pasukan Penilaian Pengajaran Prasiswazah di Fakulti

Nota: Pemantauan pencapaian objektif keselamatan maklumat di buat melalui Mesyuarat Jawatankuasa Kualiti sebanyak dua kali setahun (pertengahan dan akhir tahun) dan penilaian keseluruhan bagi tujuan penambahbaikan dibuat melalui Mesyuarat Kajian Semula Pengurusan ISMS setiap tahun.

2.4 Pihak Berkepentingan dan Keperluan Mereka

BIL.	PIHAK BERKEPENTINGAN	KEPERLUAN PIHAK BERKEPENTINGAN
1.	Pelajar	Maklumat/data peribadi dan akademik pelajar yang dilindungi
2.	Warga UPM	Maklumat/data peribadi yang dilindungi
3.	Ibubapa dan penjaga	Maklumat/data prestasi pelajar yang dilindungi
4.	Kementerian Pendidikan Malaysia (KPM)	Maklumat/data profil Universiti, pelajar, penyelidikan, sumber manusia dan kewangan yang dilindungi
5.	Penaja Pendidikan	Maklumat/data prestasi pelajar yang tepat
6.	Agensi Kerajaan	Maklumat/data yang tepat
7.	Pembekal	i. Maklumat/data kontrak yang dipatuhi ii. Maklumat/data kerjasama yang jelas
8.	Badan Penarafan	Maklumat /data yang tepat
9.	Jabatan Ketua Menteri Sarawak	Maklumat/data Universiti yang tepat
10.	Pejabat Residen Bintulu	Maklumat/data Universiti yang tepat

2.5 Isu Dalaman dan Isu Luaran

BIL.	KEBERHASILAN	ISU DALAMAN	ISU LUARAN
1.	Meningkatkan reputasi Universiti	i. Pembudayaan pengurusan keselamatan maklumat setiap warga UPM a) Kurang kefahaman dalam kalangan pekerja b) Ketidakjelasan tanggungjawab dan proses ii. Tahap kebolehpercayaan, integriti dan ketersediaan data iii. Kekangan sumber manusia dan kewangan iv. Infrastruktur tidak menyokong proses	i. Perubahan Dasar Kerajaan ii. Perkembangan teknologi dan inovasi yang pantas iii. Ekonomi tidak menentu iv. Ancaman ekologi v. Ekspektasi pelanggan terlalu tinggi vi. Kriteria penarafan yang berubah vii. Gangguan media sosial viii. Masalah komunikasi
2.	Mengekalkan status Universiti Penyelidikan (RU)		
3.	Mengekalkan status Swa Akreditasi		
4.	Mencapai kedudukan 200 universiti terbaik dunia (QS *World Ranking*) menjelang 2020		
5.	Mengekalkan status autonomi tadbir urus		
6.	Mencapai kedudukan 200 laman web universiti terbaik dalam *Webometrics Ranking* menjelang 2020		
7.	Mengekalkan kedudukan 50 universiti terbaik dalam *Green Metric*		

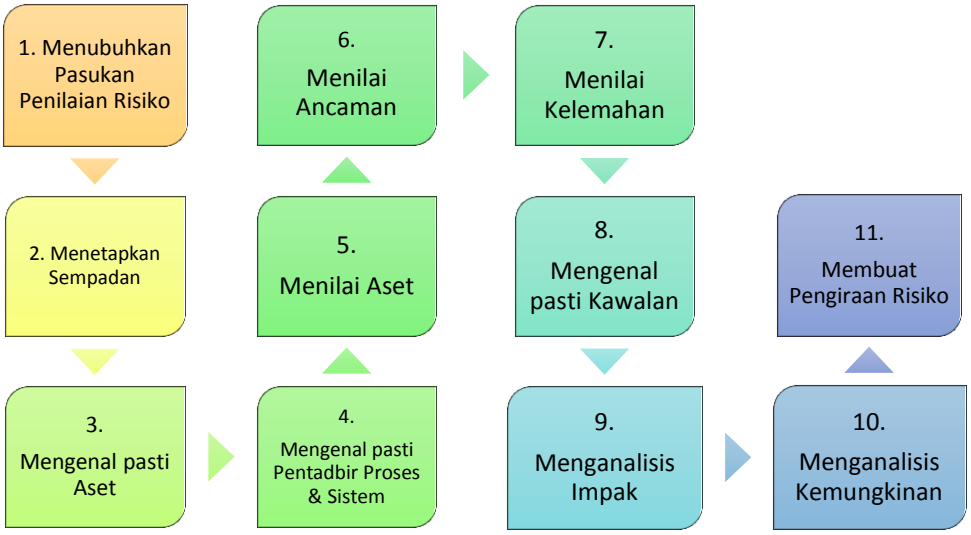
BIL.	KEBERHASILAN	ISU DALAMAN	ISU LUARAN
	World Ranking		
8.	Kebolehpasaran graduan (80% semasa konvokesyen)		
9.	Melonjakkan jaringan industri dan masyarakat		
10.	Memperkasakan UPM sebagai Pusat Kecemerlangan Pertanian		
11.	Mempertingkatkan kualiti tadbir urus		

2.6 Pengurusan Risiko

Penilaian Risiko

Penilaian risiko aset yang berkaitan dilaksanakan 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.

Sebelas (11) langkah utama dalam proses penilaian risiko aset adalah seperti berikut:



Pemulihan Risiko

Perkara yang perlu dikenalpasti dan dilaksanakan semasa proses pemulihan risiko adalah seperti berikut:

a. Membuat pilihan cadangan pemulihan risiko (menerima, mengurangkan, memindahkan, atau mengelakkan);
b. Mengenal pasti kawalan yang bersesuaian terhadap cadangan pemulihan risiko yang telah dipilih;
c. Melaksanakan perbandingan antara kawalan yang dipilih dengan Annex A;
d. Mewujudkan *Statement of Applicability (SoA)* yang mengandungi kawalan bersesuaian;
e. Menyediakan Pelan Pemulihan Risiko; dan
f. Mendapatkan kelulusan Pentadbir Proses dan Pentadbir Sistem serta penerimaan ke atas risiko yang telah dipilih.

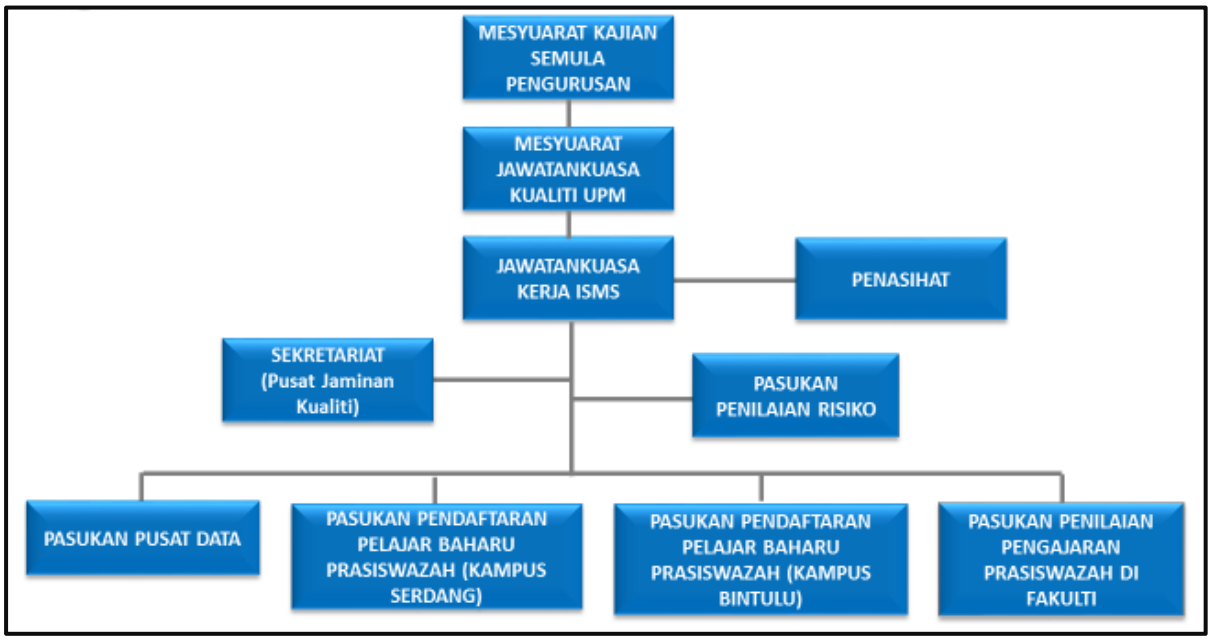
3. PENYATA PEMAKAIAN (STATEMENT OF APPLICABILITY)

Penyata Pemakaian *(Statement of Applicability)* atau SoA menjelaskan justifikasi kawalan dan dokumen rujukan dalam melindungi keselamatan aset ICT dalam skop ISMS. Pemilihan kawalan dalam SoA adalah hasil Pemulihan Risiko dan peraturan-peraturan perlindungan aset ICT dalam Kaedah-Kaedah UPM (Teknologi Maklumat dan Komunikasi) dan Garis Panduan Keselamatan Teknologi Maklumat Komunikasi (GPKTMK).

SoA terkini yang juga merupakan lampiran kepada dokumen rujukan ini boleh dirujuk melalui Portal eISO UPM di bawah pautan “Penyata Pemakaian (Statement of Applicability)”.

4. JAWATANKUASA DAN PERANAN

4.1 Struktur Organisasi ISMS



4.2 Peranan dan Tanggungjawab

PERANAN	TANGGUNGJAWAB
MESYUARAT KAJIAN SEMULA PENGURUSAN	1. Melaksanakan semakan pengurusan ke atas sistem pengurusan ISO secara berkala bagi memastikan terus sesuai, mencukupi, dan berkesan; 2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada dasar dan objektif keselamatan ISMS; dan 3. Meneliti laporan yang berkaitan dan membuat keputusan yang sesuai.
MESYUARAT JAWATANKUASA KUALITI UPM	1. Memastikan kesesuaian, kecukupan dan keberkesanan pelaksanaan Sistem Pengurusan ISO secara berkala; 2. Membuat penilaian ke atas peluang penambahbaikan dan keperluan perubahan kepada pengukuran keberkesanan ISMS; 3. Meluluskan sebarang cadangan pindaan dokumen skop pengurusan; dan 4. Mengambil maklum keberkesanan pelaksanaan ISO di peringkat Peneraju Proses dan Pusat Tanggungjawab (PTJ).
WAKIL PENGURUSAN	1. Memastikan pembangunan dan pelaksanaan ISMS mematuhi keperluan piawaian; dan 2. Melaporkan pencapaian ISMS dalam Mesyuarat Kajian Semula Pengurusan (MKSP).

PERANAN	TANGGUNGJAWAB
SEKRETARIAT PUSAT JAMINAN KUALITI	1. Merancang dan mengurus audit dalaman dan audit badan pensijilan Sistem Pengurusan ISO peringkat UPM; 2. Menyelaras dan memantau pelaksanaan tindakan penemuan audit dalaman dan audit badan pensijilan; 3. Membantu dalam Mesyuarat Jawatankuasa Kerja ISMS; dan 4. Membantu dalam pembangunan dan latihan ISMS.
JAWATANKUASA KERJA ISMS	1. Memantau keberkesanan pelaksanaan ISMS; 2. Memantau pencapaian objektif kualiti; 3. Melaksana penambahbaikan terhadap dokumentasi, proses dan perkhidmatan; 4. Menyediakan laporan keberkesanan pelaksanaan Sistem Pengurusan Keselamatan Maklumat; 5. Memantau dan menyemak carta perbatuan ISMS; 6. Membangunkan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan;* 7. Melaksanakan keputusan dan tindakan hasil Mesyuarat Kajian Semula Pengurusan ISMS; 8. Membangun dan menyelenggara pengurusan dokumen dan rekod pelaksanaan ISMS; dan 9. Mengambil tindakan ke atas kawalan ketakakuran, tindakan pembetulan dan peluang penambahbaikan.
PASUKAN PUSAT DATA, PASUKAN PENDAFTARAN PELAJAR BAHARU PRASISWAZAH (KAMPUS SERDANG DAN KAMPUS BINTULU) DAN PASUKAN PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI	1. Menyediakan analisis jurang, *Statement of Applicability* (SoA) dan prosedur berkaitan; 2. Menyediakan prosedur dan kawalan dalam ISO/IEC 27001:2013; 3. Melaksanakan penilaian risiko dan pelan pemulihan risiko; 4. Menyediakan objektif keselamatan dan kaedah pengukuran keberkesanan kawalan ISMS; 5. Mengukur keberkesanan kawalan ISMS; dan 6. Memantau dan menilai pelaksanaan ISMS. 7. Mengurus dan melaksanakan aktiviti penilaian berisiko; 8. Mengendalikan semakan semula *output* dan dokumen sebelum disampaikan kepada Penasihat Projek; 9. Menilai keputusan, menilai jurang dan menyediakan laporan *High Level Recommendation* (HLR) dan Pelan Pemulihan Risiko.

5. SENARAI *STANDARD OPERATION PROCEDURE* (SOP) YANG DIRUJUK

SOP ISMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
Dokumentasi ISMS ISO/IEC 27001 sebagaimana paparan Portal eISO UPM			
SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
1.	UPM/PGR/P001	Prosedur Pengurusan Dokumen ISO	Pusat Jaminan Kualiti
2.	UPM/PGR/P003	Prosedur Kawalan Ketakakuran, Tindakan Pembetulan, dan Peluang Penambahbaikan	Pusat Jaminan Kualiti
3.	UPM/PGR/P004	Prosedur Audit Dalaman ISO	Pusat Jaminan Kualiti
4.	UPM/PGR/P008	Prosedur Mesyuarat Kajian Semula Pengurusan ISO UPM	Pusat Jaminan Kualiti
5.	PU/PS/GP010/SMP-ID	Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar	Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik
6.	UPM/SOK/BUM/P001	Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Professional (Bukan Akademik) dan Kumpulan Pelaksana	Pejabat Pendaftar
7.	UPM/SOK/BUM/GP03/Lapor Diri	Garis Panduan Lapor Diri	Pejabat Pendaftar
8.	UPM/SOK/KEW-BUY/P016	Prosedur Perolehan Universiti	Pejabat Bursar
9.	UPM/SOK/KEW-AST/P012	Prosedur Pengurusan Aset Alih	Pejabat Bursar
10.	UPM/SOK/KEW/GP020/AST	Garis Panduan Pelupusan Aset Alih	Pejabat Bursar
11.	UPM/SOK/KEW/AK002/BUY	Arahan Kerja Penilaian Prestasi Syarikat	Pejabat Bursar
12.	UPM/SOK/LAT/P001	Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia	Pejabat Pendaftar
13.	UPM/OPR/PNC-UI/P001	Prosedur Pengurusan Mesyuarat Tatatertib Staf	Pejabat Naib Canselor (Unit Integriti)
14.	UPM/OPR/BUR-BUY/P003	Prosedur Pendaftaran Syarikat dan Pekerja/Individu	Pejabat Bursar
15.	UPM/OPR/iDEC/P001	Prosedur Pembangunan ICT	Pusat Pembangunan Maklumat dan Komunikasi
16.	UPM/OPR/iDEC/P002	Prosedur Perkhidmatan ICT	Pusat Pembangunan Maklumat dan Komunikasi
17.	UPM/OPR/iDEC/P003	Prosedur Penyelenggaraan ICT	Pusat Pembangunan Maklumat dan Komunikasi
18.	UPM/OPR/CADE/AK01	Arahan Kerja Pelaksanaan Penilaian Pengajaran	Pusat Pembangunan Akademik

SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
19.	OPR/iDEC/GP06/ Pengaturcaraan Aplikasi	Garis Panduan Perlaksanaan Pengaturcaraan Sistem Aplikasi	Pusat Pembangunan Maklumat dan Komunikasi
20.	UPM/OPR/BKU/P001	Prosedur Kawalan Akses	Bahagian Keselamatan Universiti

Kemaskini: 22 Februari 2019