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 juga 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 yang telah ditetapkan.

1.2 Sejarah Pelaksanaan ISMS di UPM

UPM telah memulakan tindakan melaksanakan ISMS dengan adanya arahan daripada Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) yang telah meminta semua Universiti Awam dipersijilkan dengan ISO/IEC 27001 supaya keselamatan maklumat terpelihara, diperoleh dengan cepat dan keselamatannya dikawal.

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. UPM telah berjaya melepasi peringkat persijilan ini dan berjaya memperolehi sijil ISMS bernombor AR5761 pada 4 Januari 2013.

Pada tahun 2018, menerusi Audit Pensijilan Semula SIRIM 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. Pada tahun yang sama, no. pensijilan ISMS UPM telah dipinda kepada ISMS 00150 berdasarkan ketetapan terkini oleh pihak SIRIM.

Pada tahun 2023, UPM sekali lagi merangka tindakan untuk memperluaskan skop pensijilan kepada Proses Pendaftaran Pelajar Baharu Sepenuh Masa Siswazah Merangkumi Aktiviti Penerimaan Tawaran Sehingga Pengesahan Pendaftaran.

2. PELAKSANAAN ISMS

2.1 Dasar ISMS

Pemakaian Dasar Sistem Pengurusan Keselamatan Maklumat (ISMS) yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

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;

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

iii. Sistem Pengurusan Keselamatan Maklumat bagi Proses Pendaftaran Pelajar Baharu Sepenuh Masa Siswazah Merangkumi Aktiviti Penerimaan Tawaran Sehingga Pengesahan Pendaftaran.

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

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

Pengecualian skop pensijilan ISMS Pendaftaran Pelajar Baharu Siswazah adalah kepada proses pendaftaran pelajar baharu siswazah untuk:

i. Pengajian Jarak Jauh; dan
ii. *Non graduating program.*

Senarai pusat tanggungjawab yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

2.3 Objektif ISMS

Penetapan Objektif ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

Nota: Pemantauan pencapaian objektif keselamatan maklumat dibuat 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

Pihak berkepentingan dan keperluan mereka yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

2.5 Isu Dalaman dan Isu Luaran

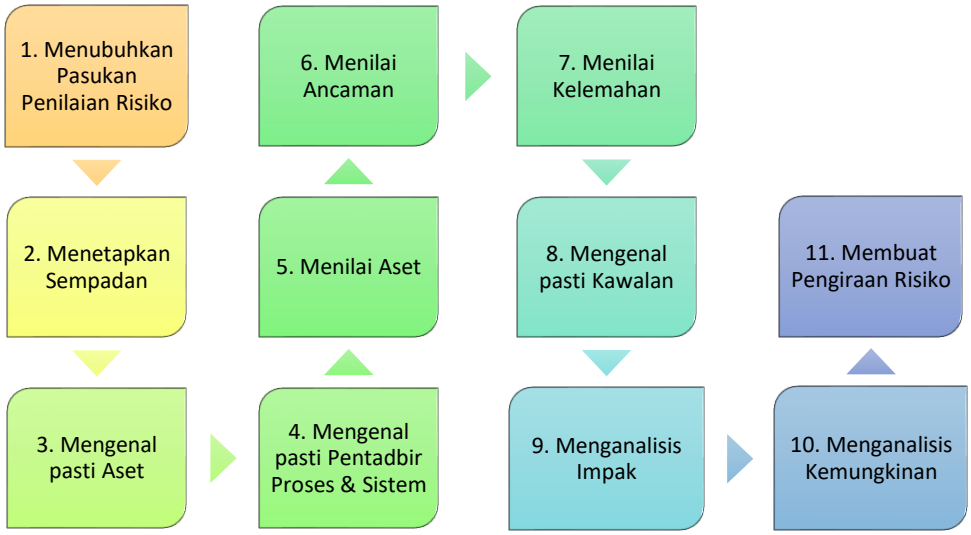
Isu dalaman dan isu luaran yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

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 Penyata Pemakaian [*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.

Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat memperincikan mengenai tatacara pengurusan penilaian risiko aset ISMS. Panduan yang juga merupakan lampiran kepada dokumen rujukan pelaksanaan ISMS ini boleh dirujuk melalui Portal eISO UPM di bawah pautan "Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat".

3. PENYATA PEMAKAIAN *[(STATEMENT OF APPLICABILITY (SOA)]*

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 Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) dan Garis Panduan Keselamatan Teknologi Maklumat dan 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 (SoA)]"*.

4. JAWATANKUASA DAN PERANAN

4.1 Struktur Organisasi ISMS

Struktur Organisasi ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

4.2 Peranan dan Tanggungjawab

Peranan dan tanggungjawab Jawatankuasa ISMS yang terkini adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (http://reg.upm.edu.my/eISO).

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.	UPM/SOK/BUM/P001	Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Profesional dan Kumpulan Pelaksana	Pejabat Pendaftar
6.	UPM/SOK/KEW-BUY/P016	Prosedur Perolehan Universiti	Pejabat Bursar
7.	UPM/SOK/KEW-AST/P012	Prosedur Pengurusan Aset Alih	Pejabat Bursar
8.	SOK/KEW/GP020/AST	Garis Panduan Pelupusan Aset Alih	Pejabat Bursar
9.	UPM/SOK/KEW/AK002/ BUY	Arahan Kerja Penilaian Prestasi Syarikat	Pejabat Bursar
10.	UPM/SOK/LAT/P001	Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia	Pejabat Pendaftar
11.	UPM/OPR/PEND/P016	Prosedur Pengurusan Mesyuarat Tatatertib Pekerja	Pejabat Pendaftar
12.	UPM/OPR/BUR-BUY/P003	Prosedur Pendaftaran Syarikat dan Pekerja/Individu	Pejabat Bursar
13.	UPM/OPR/iDEC/P001	Prosedur Pembangunan ICT	Pusat Pembangunan Maklumat dan Komunikasi
14.	UPM/OPR/iDEC/P002	Prosedur Perkhidmatan ICT	Pusat Pembangunan Maklumat dan Komunikasi

SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM			
Bil	**Kod Dokumen**	**Nama Dokumen**	**Peneraju Proses**
15.	UPM/OPR/iDEC/P003	Prosedur Penyelenggaraan ICT	Pusat Pembangunan Maklumat dan Komunikasi
16.	UPM/OPR/CADe-Lead/AK01	Arahan Kerja Pelaksanaan Penilaian Pengajaran	Pusat Pembangunan dan Kecemerlangan Kepemimpinan Akademik
17.	UPM/OPR/APSeC/P001	Prosedur Kawalan Akses	Pusat Polis Bantuan dan Keselamatan Universiti
18.	UPM/SOK/PYG/P002	Prosedur Penyelenggaraan Berkala	Pejabat Pembangunan dan Pengurusan Aset
19.	UPM/OPR/iDEC/AK31	Arahan Kerja Perkhidmatan Sokongan ICT	Pusat Pembangunan Maklumat dan Komunikasi
20.	OPR/PKU/GP13/eKlinik-ID	Garis Panduan Pengurusan Identiti Pengguna ID eKlinik	Pusat Kesihatan Universiti
21.	UPM/PU/S/P006	Prosedur Pengambilan Pelajar Siswazah	Sekolah Pengajian Siswazah

Kemaskini: 05 Oktober 2023