



**MINIT MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KE-22 (KHAS) SECARA ATAS TALIAN**

Tarikh : 01 Disember 2021 (Rabu)
Masa : 9.30 pagi
Platform : Secara atas talian menerusi aplikasi *Zoom Meeting*
Kehadiran : Seperti di **Lampiran A**

| Minit | Agenda | Tindakan/ Makluman |
|--------------|--|--|
| 22.1 | Aluan Pengerusi Pengerusi: (a) memulakan mesyuarat dengan bacaan Ummul Kitab Al-fatihah dan mengalu-alukan kehadiran ahli dan wakil yang hadir ke Mesyuarat Jawatankuasa Kerja Sistem Pengurusan Keselamatan Maklumat Kali ke-22 (Khas) secara atas talian melalui Aplikasi <i>Zoom Meeting</i> . (b) memaklumkan agenda mesyuarat pada kali ini adalah untuk membincang dan mengesahkan beberapa pelaporan untuk persediaan Audit Pensijilan Semula SIRIM ISMS Tahun 2021, iaitu: (i) Pencapaian Objektif Keselamatan Maklumat (Kemaskini November 2021); (ii) Penyata Pemakaian (SoA) Semakan Disember 2021; (iii) Dokumen Rujukan Pelaksanaan ISMS Semakan Disember 2021; (iv) Laporan Analisis Soal Selidik Pihak Berkepentingan ISMS Tahun 2021; dan (v) Persediaan Audit Pensijilan Semula SIRIM ISMS Tahun 2021. | Makluman Makluman |

| Minit | Agenda | Tindakan/ Makluman | | | | | | | | | | | | | | | | |
|-------|---|---|--|----------------------|---------------|----|---|---|--|----|---|--|--------------------|----|--|------------------------------------|---|--|
| 22.2 | <p data-bbox="316 275 855 309">Laporan Objektif Keselamatan ISMS</p> <p data-bbox="316 342 1142 414">22.2.1 Laporan Pencapaian Objektif ISMS Tahun 2021 (Kemaskini November 2021)</p> <p data-bbox="453 450 1142 622">(a) Mesyuarat mengambil maklum Laporan Pencapaian Objektif ISMS yang dikemaskini sehingga November 2021 adalah seperti Laporan Agenda 2 yang dibentangkan semasa mesyuarat.</p> <p data-bbox="453 663 1142 1081">(b) Mesyuarat mengambil maklum dua (2) objektif telah mencapai sasaran berdasarkan pengukuran semasa proses Pendaftaran Pelajar Baharu Prasiswazah yang berlaku pada 2 hingga 3 Ogos 2021 (Diploma) dan 9 hingga 10 Oktober 2021 (Bacelor) di Kampus Serdang dan Bintulu. Terdapat satu (1) objektif yang masih belum dapat diukur disebabkan proses penilaian pengajaran baru sahaja berakhir pada 30 November 2021 dan peneraju sedang dalam proses melaksanakan analisis berkaitan.</p> <p data-bbox="453 1122 1142 1227">(c) Mesyuarat mengambil maklum ringkasan pencapaian Objektif ISMS tahun 2021 yang terkini adalah seperti berikut:</p> <table border="1" data-bbox="432 1245 1139 2022"> <thead> <tr> <th data-bbox="432 1245 501 1308">Bil</th> <th data-bbox="501 1245 783 1308">Kenyataan Objektif</th> <th data-bbox="783 1245 967 1308">Sasaran & Pencapaian</th> <th data-bbox="967 1245 1139 1308">Peneraju ISMS</th> </tr> </thead> <tbody> <tr> <td data-bbox="432 1308 501 1599">1.</td> <td data-bbox="501 1308 783 1599">Memastikan pembayaran yuran pengajian adalah secara atas talian</td> <td data-bbox="783 1308 967 1599">100% (UPM Serdang)/ 100% 98% (UPM Bintulu)/ 100%</td> <td data-bbox="967 1308 1139 1599">Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Serdang dan Bintulu)</td> </tr> <tr> <td data-bbox="432 1599 501 1794">2.</td> <td data-bbox="501 1599 783 1794">Memastikan pemulihan sistem aplikasi semasa pendaftaran pelajar baharu dapat dilaksanakan</td> <td data-bbox="783 1599 967 1794">≤ 3 jam / Tiada gangguan sistem aplikasi</td> <td data-bbox="967 1599 1139 1794">Pasukan Pusat data</td> </tr> <tr> <td data-bbox="432 1794 501 2022">3.</td> <td data-bbox="501 1794 783 2022">Memastikan keyakinan pelajar terhadap keselamatan maklumat penilaian pengajaran berada pada tahap baik</td> <td data-bbox="783 1794 967 2022">80% / Belum dapat diukur</td> <td data-bbox="967 1794 1139 2022">Pasukan Penilaian Pengajaran Prasiswazah di Fakulti</td> </tr> </tbody> </table> | Bil | Kenyataan Objektif | Sasaran & Pencapaian | Peneraju ISMS | 1. | Memastikan pembayaran yuran pengajian adalah secara atas talian | 100% (UPM Serdang)/ 100% 98% (UPM Bintulu)/ 100% | Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Serdang dan Bintulu) | 2. | Memastikan pemulihan sistem aplikasi semasa pendaftaran pelajar baharu dapat dilaksanakan | ≤ 3 jam / Tiada gangguan sistem aplikasi | Pasukan Pusat data | 3. | Memastikan keyakinan pelajar terhadap keselamatan maklumat penilaian pengajaran berada pada tahap baik | 80% / Belum dapat diukur | Pasukan Penilaian Pengajaran Prasiswazah di Fakulti | <p data-bbox="1171 454 1326 488">Makluman</p> <p data-bbox="1171 658 1326 692">Makluman</p> <p data-bbox="1171 1128 1326 1162">Makluman</p> |
| Bil | Kenyataan Objektif | Sasaran & Pencapaian | Peneraju ISMS | | | | | | | | | | | | | | | |
| 1. | Memastikan pembayaran yuran pengajian adalah secara atas talian | 100% (UPM Serdang)/ 100% 98% (UPM Bintulu)/ 100% | Pasukan Pendaftaran Pelajar Baharu Prasiswazah (Serdang dan Bintulu) | | | | | | | | | | | | | | | |
| 2. | Memastikan pemulihan sistem aplikasi semasa pendaftaran pelajar baharu dapat dilaksanakan | ≤ 3 jam / Tiada gangguan sistem aplikasi | Pasukan Pusat data | | | | | | | | | | | | | | | |
| 3. | Memastikan keyakinan pelajar terhadap keselamatan maklumat penilaian pengajaran berada pada tahap baik | 80% / Belum dapat diukur | Pasukan Penilaian Pengajaran Prasiswazah di Fakulti | | | | | | | | | | | | | | | |

| Minit | Agenda | Tindakan/ Makluman |
|-------|--|---|
| 22.3 | <p>(d) Mesyuarat bersetuju mengesahkan laporan pencapaian objektif ISMS kemaskini November 2021 dengan cadangan supaya penulisan maklumat pencapaian bagi objektif ISMS 'Memastikan pembayaran yuran pengajian adalah secara atas talian' ditambahbaik supaya lebih menampakkan elemen keselamatan maklumat yang ingin dikawal.</p> | TWP ISMS & Penyelaras ISMS |
| | <p>(e) Mesyuarat meminta peneraju Penilaian Pengajaran Prasiswazah di Fakulti menyediakan draf pencapaian objektif ISMS bagi Proses Penilaian Pengajaran Prasiswazah Semester Kedua 2020/2021 sebagai persediaan data untuk Audit SIRIM ISMS Tahun 2021.</p> | Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti |
| | <p>(f) Mesyuarat dimaklumkan bahawa satu sesi semakan dan penambahbaikan menyeluruh ke atas objektif keselamatan maklumat akan dilaksanakan pada sukuan pertama tahun 2022 mengambilkira penemuan audit dalaman tahun 2021 serta keperluan terkini pelaksanaan Sistem Pengurusan Keselamatan Maklumat di UPM. Perincian mengenainya akan dimaklumkan kemudian oleh pihak Urusetia CQA kepada semua pasukan/entiti ISMS yang terlibat.</p> | Penyelaras ISMS |
| | <p>Laporan Penyata Pemakaian (Statement of Applicability) & Dokumentasi ISMS</p> <p>22.3.1 Laporan Penyata Pemakaian (SoA) Semakan Disember 2021</p> <p>(a) Mesyuarat mengambil maklum perubahan Penyata Pemakaian (SoA) semakan Disember 2021 adalah sebagaimana dalam Laporan Agenda 3 yang dibentang melibatkan perkara berikut:</p> <p>(i) penstrukturan semula entiti Bahagian Governan dan Integriti, Pejabat Naib Canselor kepada Bahagian Governan dan Integriti, Pejabat Pendaftar;</p> <p>(ii) kemaskini senarai dokumentasi ISO terkini;</p> | Makluman |

| Minit | Agenda | Tindakan/ Makluman |
|-------|--|--|
| | <p>dan</p> <p>(iii) penambahbaikan hasil audit dalaman tahun 2021.</p> <p>(b) Mesyuarat bersetuju meluluskan cadangan penambahbaikan SoA semakan Disember 2021 sebagaimana yang dinyatakan pada Lampiran B untuk dikuatkuasakan pemakaiannya bermula 01 Disember 2021. Mesyuarat turut meminta supaya pemakaian dokumen SoA yang terkini dihebahkan kepada semua peneraju/entiti yang terlibat dengan pelaksanaan ISMS di UPM.</p> <p>22.3.2 Dokumen Rujukan Pelaksanaan ISMS Semakan Disember 2021</p> <p>(a) Mesyuarat mengambil maklum perubahan Dokumen Rujukan Pelaksanaan ISMS semakan Disember 2021 adalah sebagaimana Laporan Agenda 3 yang dibentang iaitu turut melibatkan:</p> <p>(i) penstrukturan semula entiti Bahagian Governan dan Integriti, Pejabat Naib Canselor kepada Bahagian Governan dan Integriti, Pejabat Pendaftar;</p> <p>(ii) kemaskini senarai dokumentasi ISO terkini; dan</p> <p>(iii) penambahbaikan hasil audit dalaman tahun 2021.</p> <p>(b) Mesyuarat meneliti dan bersetuju meluluskan perubahan Dokumen Rujukan Pelaksanaan ISMS semakan Disember 2021 sebagaimana yang dinyatakan pada Lampiran C. Dokumen ini akan dikuatkuasakan pemakaiannya pada 01 Disember 2021 dan perlu dihebahkan pemakaiannya kepada semua peneraju/ entiti ISMS di UPM.</p> | <p>Penyelaras ISMS</p> <p>Makluman</p> <p>Penyelaras ISMS</p> |
| 22.4 | <p>Hal-hal Lain</p> <p>22.4.1 Laporan Analisis Pelaksanaan Soal Selidik Pihak Berkepentingan ISMS Tahun 2021</p> <p>(a) Mesyuarat mengambil maklum Laporan Analisis</p> | <p>Makluman</p> |

| Minit | Agenda | Tindakan/ Makluman |
|-------|---|---|
| | <p>(d) Mesyuarat dimaklumkan semakan ke atas soal soal selidik pihak berkepentingan ISMS akan dibuat sebelum pelaksanaan Soal Selidik Pihak Berkepentingan ISMS tahun 2022 berdasarkan cadangan penambahbaikan semasa Mesyuarat Kajian Semula Pengurusan UPM tahun 2021.</p> <p>(e) Mesyuarat mengambil maklum bahawa Laporan Analisis Soal Selidik Keselamatan Maklumat bagi proses Penilaian Pengajaran Prasiswazah Semester Kedua 2020/2021 masih dalam proses tindakan peneraju Pusat Pembangunan Akademik.</p> <p>(f) Mesyuarat meminta supaya draf Laporan Analisis Soal Selidik Keselamatan Maklumat bagi proses Penilaian Pengajaran Prasiswazah Semester Kedua 2020/2021 turut disediakan oleh peneraju sebagai persediaan menghadapi audit pensijilan semula SIRIM tahun 2021. Pengesahan laporan penuh akan dibuat pada mesyuarat akan datang.</p> <p>22.4.2 Persediaan Audit Pensijilan Semula SIRIM ISMS Tahun 2021</p> <p>Mesyuarat mengambil maklum:</p> <p>(a) Audit Pensijilan Semula SIRIM ISMS Tahun 2021 akan dilaksana pada 13 hingga 17 Disember 2021, melibatkan seramai dua (2) orang Juruaudit SIRIM yang diketuai oleh Puan Nur Eliana Abdul Razak. Perinciannya adalah sepertimana jadual audit yang dibentangkan di bawah Laporan Agenda 4.2;</p> <p>(b) sebanyak 17 PTJ terpilih menjadi sampel audit ISMS SIRIM pada kali ini; dan</p> <p>(c) perincian persediaan yang perlu dilaksana oleh semua PTJ yang menjadi sampel audit tahun 2021 akan dimaklumkan oleh pihak CQA semasa Sesi Taklimat Persediaan Audit SIRIM secara maya pada 7 Disember 2021.</p> | <p>Makluman</p> <p>Makluman</p> <p>Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti</p> <p>Makluman</p> <p>Makluman</p> <p>Makluman</p> |

**SENARAI KEHADIRAN
MESYUARAT JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013 KALI KE-22 (KHAS) SECARA ATAS TALIAN**

HADIR

1. Ts. Shahril Iskandar Amir (Timbalan Wakil Pengurusan ISMS) - **Pengerusi**
2. Encik Rosmi Othman (Penasihat Jawatankuasa Kerja ISMS)
3. Encik Shahrman Hashim (Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)
4. Encik Sudirman Asmadi (Timbalan Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu)
5. Ts. Mohamad Farid Harun (Ketua, Pasukan Pusat Data)
6. Ts. Rostam Abu Bakar (Timbalan Ketua, Pasukan Pusat Data)
7. Puan Yasminani Mohamad (Timbalan Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti)
8. Encik Wan Hafizi Wan Umar (Penyelaras Penilaian Risiko ISMS)
9. Puan Shamriza Shari (Penyelaras ISMS) - **Setiausaha**

TURUT HADIR

1. Encik Adidi Tamin (Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)
2. Encik Mohd Amaludin Salleh (Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu)
3. Puan Fairuz Muchtar (Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik)
4. Puan Kasmaria Zawawi (Pusat Jaminan Kualiti)

TIDAK HADIR (DENGAN KENYATAAN)

1. Dato' Haji Rosdi Wah (Penasihat Jawatankuasa Kerja ISMS)
2. Ts. Mohd Faizal Daud (Penasihat Jawatankuasa Kerja ISMS)
3. Puan Haslida Hassan (Penasihat Jawatankuasa Kerja ISMS)
4. Encik Nuruliman Ibrahim (Timbalan Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang)
5. Encik Noor Hakim Ahmad (Ketua, Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu)
6. Encik Ahmad Nizam Abdullah (Ketua, Pasukan Penilaian Pengajaran Prasiswazah di Fakulti)



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

1.0 PENGENALAN

Dokumen Penyata Pemakaian (*Statement of Applicability (SoA)*) menggariskan objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013 selaras dengan keperluan Sistem Pengurusan Keselamatan Maklumat di Universiti Putra Malaysia.

2.0 TUJUAN

Dokumen ini bertujuan untuk menetapkan proses yang perlu dipatuhi dalam menyediakan SoA.

3.0 PROSES PENYATA PEMAKAIAN (SoA)

3.1 PENYEDIAAN SoA

Proses yang terlibat dalam penyediaan SoA merangkumi:

- (a) Memahami keperluan SoA dalam Standard MS ISO/IEC 27001:2013.
- (b) Menyediakan kandungan SoA dengan mengambil kira aspek berikut:
 - (i) Menyenaraikan semua objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013;
 - (ii) Memberi jawapan "**Ya**" dengan justifikasi pemilihan kepada objektif kawalan dan kawalan selaras dengan **penemuan Pelan Pemulihan Risiko**;
 - (iii) Memberi jawapan "**Ya**" kepada objektif kawalan dan kawalan **yang sedang dilaksanakan**;
 - (iv) Memberi jawapan "**Separa**" kepada kawalan yang **masih dalam pembangunan**;
 - (v) Menyenaraikan **nama prosedur / panduan / dokumen** yang dirujuk bagi menyokong pelaksanaan objektif kawalan dan kawalan tersebut; dan
 - (vi) Memberi jawapan "**Tidak**" kepada objektif kawalan dan kawalan yang **tidak dipilih** dengan alasan pengecualiannya.
- (c) Membentangkan cadangan awal SoA dalam Mesyuarat Jawatankuasa Kerja ISMS.

3.2 PELAKSANAAN SoA

Pelaksanaan SoA hendaklah mengambil kira aspek berikut:

- (a) Memaklumkan kepada semua pengguna ISMS berhubung penguatkuasaan dokumen SoA;
- (b) Melaksanakan program kesedaran pematuhan semua peraturan Polisi ISMS selaras dengan keperluan SoA;



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

- (c) Memantau tahap pematuhan pelaksanaan kawalan dalam SoA sekurang-kurangnya sekali dalam setahun; dan
- (d) Melaporkan penemuan di para c) dalam Mesyuarat Jawatankuasa Kerja ISMS untuk pertimbangan dan kelulusan.

3.3 PENGEMASKINIAN SoA

SoA perlu dikemaskini dengan mengambilkira perkara berikut:

- (a) Penemuan penilaian semula risiko;
- (b) Perubahan justifikasi pemilihan kawalan;
- (c) Perluasan skop ISMS;
- (d) Penambahan atau pengecualian aset ISMS;
- (e) Perubahan struktur organisasi;
- (f) Penambahbaikan ke atas pelaksanaan ISMS;
- (g) Pengemaskinian ke atas dokumen rujukan; dan
- (h) Perubahan disebabkan oleh keperluan lain.

Sebarang pindaan kepada SoA hendaklah mematuhi perkara yang dinyatakan dalam para 3.1(c) di atas.

4.0 JADUAL PENYATAAN PEMAKAIAN (SoA)

SoA di **LAMPIRAN A** menyediakan ringkasan keputusan berkaitan pemulihan risiko (*risk treatment*). Sebarang objektif kawalan dan kawalan yang **tidak dipilih** diberikan alasan pengecualiannya bagi memastikan suatu kawalan tidak sengaja diabaikan.



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

Lampiran A: SoA Pensijilan MS ISO/IEC 27001:2013 ISMS Universiti Putra Malaysia

| Kawalan ISO/IEC 27001:2013 | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa | |
|---|---------|---|-----------------------|--------------------------------|-------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.5 DASAR KESELAMATAN MAKLUMAT | A.5.1 | Hala tuju pengurusan untuk keselamatan maklumat Menyediakan hala tuju dan sokongan pengurusan untuk keselamatan maklumat menurut keperluan perniagaan serta undang-undang dan peraturan yang berkaitan. | | | | | |
| | A.5.1.1 | Dasar keselamatan maklumat Satu set dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan dan disampaikan kepada kakitangan dan pihak luaran yang berkaitan. | Pusat Jaminan Kualiti | YA | YA | Memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum. | <ul style="list-style-type: none"> Dasar ISMS UPM <ul style="list-style-type: none"> - diluluskan oleh Pengerusi Lembaga Pengarah Universiti - dikomunikasi menerusi Portal eISO UPM |
| | A.5.1.2 | Kajian semula dasar untuk keselamatan maklumat Dasar untuk keselamatan maklumat hendaklah dikaji semula pada sela masa yang dirancang atau jika berlaku perubahan yang ketara bagi memastikan kesesuaian, kecukupan dan keberkesannya berterusan. | Pusat Jaminan Kualiti | YA | YA | Memastikan dasar sentiasa terkini berdasarkan skop dan pelaksanaan ISMS. | <ul style="list-style-type: none"> Semakan berkala dilaksanakan semasa Mesyuarat Kajian Semula Pengurusan ISMS UPM |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|--|---------|--|-----------------------------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.6 PERANCANGAN BAGI KESELAMATAN MAKLUMAT | A.6.1 | Perancangan dalaman Menyediakan rangka kerja pengurusan untuk memulakan dan mengawal pelaksanaan dan operasi keselamatan dalam organisasi. | | | | | |
| | A.6.1.1 | Peranan dan tanggungjawab keselamatan maklumat Semua tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan. | Pusat Jaminan Kualiti | YA | YA | Memastikan semua tanggungjawab keselamatan maklumat ditakrifkan dan diperuntukkan. | <ul style="list-style-type: none"> Peranan dan Tanggungjawab Jawatankuasa Keselamatan Maklumat UPM - menerusi Portal eISO UPM |
| | A.6.1.2 | Pengasingan tugas Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah, atau menyalahgunakan aset organisasi. | Peneraju ISMS & Pejabat Pendaftar | YA | YA | Memastikan tugas dan bidang tugas diasingkan untuk mengurangkan peluang bagi pengubahsuaian atau penyalahgunaan aset organisasi yang tidak dibenarkan atau yang tidak disengajakan. | <ul style="list-style-type: none"> Senarai tugas Akademik/Bukan Akademik/Pelaksana <ul style="list-style-type: none"> Termasuk tugas pentadbiran. (Contoh: sebagai Dekan, Pengetua Kolej, Pengarah, Penolong Pengarah/Timbangan Pengarah) Senarai tugas pada setiap pekerja UPM Struktur organisasi PTJ |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|----------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.6.1.3 | Hubungan dengan pihak berkuasa Hubungan yang baik dengan pihak berkuasa yang berkaitan hendaklah dikekalkan. | Peneraju ISMS | YA | YA | Memastikan hubungan dengan pihak berkuasa berkaitan dikekalkan. | <ul style="list-style-type: none"> Akta Universiti dan Kolej Universiti 1971 Akta Perubatan 1971 Akta Perlesenan Tenaga Atom 1984 (Akta 304) Seksyen 66 Akta Imigresen 1969/63 (Akta 155) Perlembagaan Universiti Putra Malaysia (P.U.(A) 448/2010) Malaysian Medical Council |
| | A.6.1.4 | Hubungan dengan kumpulan berkepentingan yang khusus Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan persatuan/pertubuhan profesional yang lain hendaklah dikekalkan. | Peneraju ISMS | YA | YA | Memastikan hubungan dengan pihak kepentingan atau lain-lain forum keselamatan dan persatuan profesional dikekalkan. | <ul style="list-style-type: none"> Pelan Kesinambungan Perkhidmatan (PKP) Pelan Komunikasi Krisis Prosedur Garis Panduan Pelan Tindak Balas Insiden ICT-(UPM/ISMS/SOK/P001) (IDEC/ISMS/GP02) Pelan Pemulihan Bencana ICT (Rujukan DRP ICT UPM) Pengauditan OSHA MyCert Cybersecurity Malaysia |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|---|---------------------|--------------------------------|--|--|
| Klasua | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.6.1.5 | Keselamatan maklumat dalam pengurusan projek Keselamatan maklumat hendaklah ditangani dalam pengurusan projek, tanpa mengambil kira jenis projek. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan keselamatan maklumat dalam pengurusan projek yang terlibat dalam skop pensijilan dikawal. | <ul style="list-style-type: none"> Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) Garis Panduan Pelaksanaan Implementasi Aplikasi (OPR/IDEC/GP07/IMPLEMENTASI APLIKASI) (IDEC/PEM/GP02) |
| | A.6.2 | Peranti mudah alih dan telekerja Memastikan keselamatan telekerja dan penggunaan peranti mudah alih. | | | | | |
| | A.6.2.1 | Dasar peranti mudah alih Dasar dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi menguruskan risiko yang timbul melalui penggunaan peranti mudah alih. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan polisi dan sokongan kepada pengukuran keselamatan diambil kira bagi mengurus risiko daripada penggunaan peranti mudah alih. | <ul style="list-style-type: none"> GPKTMK 6.2.1 Peranti Mudah Alih Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH) |
| | A.6.2.2 | Telekerja Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di tapak telekerja. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawalan capaian kepada sistem (teleworking) oleh pekerja yang dibenarkan sahaja. | <ul style="list-style-type: none"> Garis Panduan Pemantauan Capaian ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) GPKTMK 6.2.2 <i>Teleworking</i> Arahan Kerja Perkhidmatan Sokongan ICT (OPR/IDEC/AK31/PERKHIDMATAN SOKONGAN ICT) Perkara 3.2.1 Rangkaian |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|---|---------|--|-------------------|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.7 KESELAMATAN SUMBER MANUSIA | A.7.1 | Sebelum penjawatan Memastikan kakitangan dan kontraktor memahami tanggungjawab mereka dan sesuai dengan peranan yang dipertimbangkan untuk mereka. | | | | | |
| | A.7.1.1 | <p>Saringan Semakan penentusahan latar belakang ke atas semua calon untuk penjawatan hendaklah dilakukan menurut undang-undang, peraturan dan etika yang berkaitan dan hendaklah bersesuaian dengan keperluan perniagaan, klasifikasi maklumat yang hendak diakses dan risiko yang dikenal pasti.</p> | Pejabat Pendaftar | YA | YA | Memastikan semua calon melepasi tapisan keselamatan Kerajaan Malaysia bagi semua calon yang ditawarkan jawatan di UPM. | <ul style="list-style-type: none"> Prosedur Pelantikan Staf Tetap Bagi Kumpulan Pengurusan dan Profesional (Bukan Akademik) dan Kumpulan Pelaksana (UPM/SOK/BUM/P001) GPCTMK 7.0 (a) : Sebelum Perkhidmatan Surat Tawaran Jawatan Tetap – keperluan tapisan keselamatan KERAJAAN MALAYSIA. Ini dilaksanakan secara dalam talian di http://evetting.cgso.gov.my/ dalam tempoh 30 hari mulai tarikh lapor diri. Bukti permohonan tapisan keselamatan kerajaan Malaysia telah dibuat dikemukakan kepada Pejabat Pendaftar semasa melapor diri. Rekod Kenyataan Perkhidmatan (RKP) bagi calon yang dilantik dari agensi luar |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|------------------------------------|---------------------|--------------------------------|--|---|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.7.1.2 | Terma dan syarat penjawatan Persetujuan berkontrak dengan kakitangan dan kontraktor hendaklah menyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. | Pejabat Pendaftar & Pejabat Bursar | YA | YA | Memastikan kontrak perjanjian terhadap pekerja dan pembekal menyatakan tanggungjawab organisasi terhadap keselamatan maklumat. | <ul style="list-style-type: none"> Prosedur Pendaftaran Syarikat dan Pekerja/Individu (UPM/OPR/BUR-BUY/P003) Surat Aku Janji Borang Pengesahan Laporan Diri (SOK/BUM/BR03/BORANGPENGESEAHAN) Borang Perakuan untuk ditandatangani Oleh penjawat Awam Berkenaan Dengan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI) |
| | A.7.2 | Dalam tempoh penjawatan Memastikan kakitangan dan kontraktor mengetahui dan memenuhi tanggungjawab keselamatan maklumat mereka. | | | | | |
| | A.7.2.1 | Tanggungjawab pengurusan Pengurusan hendaklah menghendaki semua kakitangan dan kontraktor supaya mengamalkan keselamatan maklumat menurut dasar dan prosedur organisasi yang ditetapkan. | Pejabat Pendaftar & Pejabat Bursar | YA | YA | Memastikan polisi dan prosedur keselamatan maklumat yang telah ditetapkan oleh organisasi diikuti oleh pekerja dan pembekal. | <ul style="list-style-type: none"> Perintah Am Peraturan Kewangan Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) Surat Aku Janji Borang Perakuan untuk Ditandatangani oleh Penjawat Awam Berkenaan Akta Rahsia Rasmi 1972 (SOK/BUM/BR03/AKTA RAHSIA RASMI) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.7.2.2 | Kesedaran, pendidikan dan latihan tentang keselamatan maklumat Semua kakitangan organisasi dan, jika berkaitan, kontraktor hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya dan menerima maklumat secara tetap tentang dasar dan prosedur organisasi, yang berkaitan dengan fungsi tugas mereka. | Peneraju ISMS (Pasukan pendaftaran Pelajar Baharu Prasiswazah – Kampus Serdang & Pasukan Pusat Data), Pejabat Pendaftar, Pejabat Bursar & Pusat Jaminan Kualiti | YA | YA | Memastikan pekerja, pelajar dan pembekal menerima latihan dan program kesedaran berkaitan dengan polisi organisasi yang berkaitan dengan fungsi kerja masing-masing. | <ul style="list-style-type: none"> Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia (UPM/SOK/LAT/P001) GPkTMK Perkara 7.2 (b) Dalam Perkhidmatan Taklimat Keselamatan Maklumat bagi Pelaksanaan Minggu Perkasa Putra ISMS – Latihan/Takwim di bawah Pusat Jaminan Kualiti Surat Aku Janji Pihak Luar |
| | A.7.2.3 | Proses tatatertib Proses tatatertib yang formal hendaklah diadakan dan disampaikan kepada kakitangan bagi membolehkan tindakan diambil terhadap mereka yang melakukan pelanggaran keselamatan maklumat. | Pejabat Pendaftar & Unit Integriti, Pejabat Naib Canselor | YA | YA | Memastikan proses tindakan tatatertib dilaksanakan terhadap pekerja yang telah melanggar peraturan keselamatan maklumat. | <ul style="list-style-type: none"> Akta 605 - Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 Akta Rahsia Rasmi 1972 Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F Prosedur Pengurusan Mesyuarat Tatatertib Staf Pekerja (UPM/OPR/PNC-U/P001) (UPM/OPR/PEND/P016) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|------------------------------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.7.3 | Penamatan dan pertukaran penjawatan Melindungi kepentingan organisasi sebagai sebahagian daripada proses pertukaran atau penamatan penjawatan. | | | | | |
| | A.7.3.1 | Penamatan atau pertukaran tanggungjawab penjawatan Tanggungjawab dan tugas keselamatan maklumat yang masih sah selepas penamatan atau pertukaran penjawatan hendaklah ditakrifkan, disampaikan kepada kakitangan dan kontraktor dan dikuatkuasakan. | Pejabat Pendaftar & Pejabat Bursar | YA | YA | Memastikan tanggungjawab keselamatan maklumat terhadap pekerja atau pembekal yang telah tamat perkhidmatan atau berlaku perubahan pekerja hendaklah dikenal pasti dan dikuatkuasakan. | <ul style="list-style-type: none"> Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2012 GPKTMK Perkara 7.0 (C) Bertukar Atau Tamat Perkhidmatan Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS) Dokumen Perjanjian dengan Pembekal/Kontraktor/Pihak Ketiga |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|--------------------------------|---------|--|--------------------------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.8 PENGURUSAN ASET | A.8.1 | Tanggungjawab terhadap aset Mengenal pasti aset organisasi dan mentakrifkan tanggungjawab perlindungan yang sewajarnya. | | | | | |
| | A.8.1.1 | Inventori aset Maklumat, lain-lain aset yang dikaitkan dengan maklumat, dan fasiliti pemprosesan maklumat hendaklah dikenal pasti dan inventori aset ini hendaklah disediakan dan disenggarakan. | Peneraju ISMS & Pejabat Bursar | YA | YA | Memastikan aset yang terlibat dengan fasiliti pemprosesan maklumat dikenalpasti dan inventori aset tersebut sedia dan diselenggara. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014 Bahagian D GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) |
| | A.8.1.2 | Pemilikan aset Aset yang disenggara dalam inventori hendaklah mempunyai pemilik. | Peneraju ISMS & Pejabat Bursar | YA | YA | Memastikan setiap aset yang diselenggara mempunyai pemilik. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D GPKTMK 3.0 Perkara 8.0 : Pengurusan Aset Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.8.1.3 | Penggunaan aset yang dibenarkan Peraturan penggunaan yang dibenarkan bagi maklumat dan aset yang dikaitkan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti, didokumenkan dan dilaksanakan. | Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan peraturan untuk kebolehgunaan maklumat dan aset yang berkaitan dengan kemudahan pemprosesan maklumat dan maklumat itu dikenal pasti, didokumen dan dilaksanakan. | <ul style="list-style-type: none"> • Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F • GPKTMK 3.0 Perkara 8.2 Pengelasan dan Pengendalian Maklumat |
| | A.8.1.4 | Pemulangan aset Semua kakitangan dan pengguna pihak luar hendaklah memulangkan semua aset organisasi yang berada dalam pemilikannya apabila ditamatkan penjawatan, kontrak atau perjanjian mereka. | Peneraju ISMS, Pejabat Pendaftar & Pejabat Bursar | YA | YA | Memastikan aset organisasi dipulangkan selepas tamat perkhidmatan. | <ul style="list-style-type: none"> • Perintah –perintah Am Persekutuan Bab A : Peraturan-Peraturan Pegawai Awam (Pelantikan, Kenaikan Pangkat Dan Penamatan Perkhidmatan) 2012 • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • Pekerja : Borang Nota Serah Tugas (SOK/BUM/BR03/SERAH TUGAS) • Dokumen Kontrak Perolehan Pembekal/Pihak Ketiga • Surat Pertukaran (pekerja tidak lagi boleh mengakses sistem di PTJ lama) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|-----------------------------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.8.2 | Pengelasan maklumat Memastikan maklumat mendapat tahap perlindungan yang sesuai menurut kepentingannya kepada organisasi. | | | | | |
| | A.8.2.1 | Pengelasan maklumat Maklumat hendaklah dikelaskan berdasarkan keperluan undang-undang, nilai, tahap kritikal dan sensitiviti terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan. | Peneraju ISMS & Pejabat Pendaftar | YA | YA | Memastikan maklumat dikelaskan untuk mengelak daripada pendedahan atau pengubahsuaian yang tidak dibenarkan. | <ul style="list-style-type: none"> Arahan Keselamatan Kerajaan Malaysia Akta Arkib Negara 2003 (Akta 629) GPKTMK 3.0 Perkara 8.2 Pengelasan dan Pengendalian Maklumat Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |
| | A.8.2.2 | Pelabelan maklumat Set prosedur yang sesuai untuk pelabelan maklumat hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi. | Peneraju ISMS & Pejabat Pendaftar | YA | YA | Memastikan prosedur untuk pelabelan maklumat dibangunkan mengikut skema klasifikasi maklumat oleh organisasi. | <ul style="list-style-type: none"> Arahan Keselamatan Kerajaan Malaysia Akta Arkib Negara 2003 (Akta 629): (m/s : 28) Bahagian V: Pentadbiran Arkib-Pemprosesan dan pemeliharaan arkib awam. GPKTMK 3.0 Perkara 8.2 Pengelasan dan Pengendalian Maklumat Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|----------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.8.2.3 | Pengendalian aset Prosedur pengendalian aset hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi. | Peneraju ISMS | YA | YA | Memastikan prosedur pengendalian aset dibangunkan dan dilaksanakan mengikut skema klasifikasi maklumat oleh organisasi. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D • GPKTMK 3.0 Perkara 8.0 Pengurusan Aset • Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |
| | A.8.3 | Pengendalian media Mencegah pendedahan, pengubahsuaian, penyingkiran, atau pemusnahan tanpa kebenaran terhadap maklumat yang disimpan dalam media. | | | | | |
| | A.8.3.1 | Pengurusan media boleh alih Prosedur hendaklah dilaksanakan bagi pengurusan media boleh alih menurut skim pengelasan maklumat yang diterima pakai oleh organisasi. | Peneraju ISMS | YA | YA | Memastikan prosedur bersesuaian dibangunkan mengikut klasifikasi yang digunakan oleh organisasi. | <ul style="list-style-type: none"> • Tatacara Pengurusan Aset Alih Kerajaan : Pelupusan • GPKTMK 3.0 Perkara 8.3 : Pengendalian media • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|----------------|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.8.3.2 | Pelupusan media Media hendaklah dilupuskan dengan selamat melalui prosedur formal apabila tidak diperlukan lagi. | Peneraju ISMS | YA | YA | Media yang tidak lagi diperlukan perlu dilupuskan menggunakan prosedur yang dibangunkan. | <ul style="list-style-type: none"> Tatacara Pengurusan Aset Alih Kerajaan : Pelupusan GPKTMK 3.0 Perkara 8.3 : Pengendalian media Arahan Kerja Pelupusan Pita <i>Backup</i> dan Lain-lain Media Simpanan (UPM/ISMS/OPR/AK07) Garis Panduan Pelupusan Aset Alih (UPM/SOK/KEW/GP020/AST) |
| | A.8.3.3 | Pemindahan media fizikal Media yang mengandungi maklumat hendaklah dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa pengangkutan. | Peneraju ISMS | YA | YA | Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa perpindahan. | <ul style="list-style-type: none"> GPKTMK 3.0 Perkara 8.3 – Pengendalian Media Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|------------------------------|---------|---|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.9 KAWALAN AKSES | A.9.1 | Kawalan akses bagi keperluan perniagaan Mengehadkan akses kepada maklumat dan kemudahan pemrosesan maklumat. | | | | | |
| | A.9.1.1 | Dasar kawalan akses Dasar kawalan akses hendaklah diwujudkan, didokumenkan dan dikaji semula berdasarkan keperluan perniagaan dan keperluan keselamatan maklumat. | Peneraju ISMS | YA | YA | Dasar kawalan capaian hendaklah diwujudkan, didokumen dan dikaji semula berdasarkan keperluan keselamatan perniagaan dan maklumat. | <ul style="list-style-type: none"> Arahan Keselamatan : Keselamatan Fizikal GPKTMK 3.0 Perkara 9.1 : Dasar Kawalan Akses Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) |
| | A.9.1.2 | Akses kepada rangkaian dan perkhidmatan rangkaian Pengguna hanya hendaklah diberikan akses kepada rangkaian dan perkhidmatan rangkaian yang dibenarkan secara khusus. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pengguna mempunyai akses kepada perkhidmatan rangkaian yang telah dikhususkan kepada mereka. | <ul style="list-style-type: none"> GPKTMK 3.0 Perkara 13.2 : Kawalan Akses Rangkaian Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|----------------|---------------------|--------------------------------|---|--|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.9.2 | Pengurusan akses pengguna Memastikan akses oleh pengguna yang dibenarkan dan menghalang akses tanpa izin kepada sistem dan perkhidmatan. | | | | | |
| | A.9.2.1 | Pendaftaran dan pembatalan pengguna Proses formal pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan pemberian hak akses. | Peneraju ISMS | YA | YA | Memastikan proses pendaftaran dan pembatalan pengguna dilaksanakan untuk membolehkan pemberian hak akses. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|----------------|---------------------|--------------------------------|--|---|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.9.2.2 | Peruntukan akses pengguna Proses formal peruntukan akses pengguna hendaklah dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna untuk semua sistem dan perkhidmatan. | Peneraju ISMS | YA | YA | Memastikan penetapan dan pembatalan hak akses untuk semua jenis pengguna dilaksanakan. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti |
| | A.9.2.3 | Pengurusan hak akses istimewa Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. | Peneraju ISMS | YA | YA | Memastikan kebenaran hak akses dihadkan dan dikawal. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | | | | | | <ul style="list-style-type: none"> • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) • Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti |
| | A.9.2.4 | Pengurusan maklumat pengesahan rahsia pengguna Peruntukan maklumat pengesahan rahsia hendaklah dikawal melalui proses pengurusan formal. | Peneraju ISMS, Pejabat Pendaftar & Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik | YA | YA | Memastikan pengesahan maklumat rahsia sentiasa dikawal. | <ul style="list-style-type: none"> • GPKTMK 3.0 Perkara 10.0 : Kawalan Kriptografi • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • Kelulusan Ketua Bahagian Pengurusan Sumber Manusia bagi permohonan baru/ kemaskini bagi perolehan ID eIHRAMS. |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|---|---------------------|--------------------------------|---|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | | | | | | <ul style="list-style-type: none"> Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) - Perkara 2.0.8 Nyahaktif Akaun UPM-ID |
| | A.9.2.5 | Kajian semula hak akses pengguna Pemilik aset hendaklah mengkaji semula hak akses pengguna pada sela masa tetap. | Peneraju ISMS, Pejabat Bursar & Pejabat Pendaftar | YA | YA | Memastikan hak capaian pengguna disemak semula. | <ul style="list-style-type: none"> Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) Semakan semula ID pengguna eIHRAMS dilaksanakan setahun sekali Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|--|----------------|---------------------|--------------------------------|---|---|
| Klasua | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.9.2.6 | <p>Penyingkiran atau palarasan hak akses Hak akses semua kakitangan dan pengguna pihak luar kepada maklumat dan kemudahan pemprosesan maklumat hendaklah disingkirkan apabila ditamatkan penjawatan, kontrak atau perjanjian, atau diselaraskan apabila terdapat perubahan.</p> | Peneraju ISMS | YA | YA | Memastikan hak akses kepada maklumat dan kemudahan dikeluarkan selepas tamat perkhidmatan atau apabila berlaku perubahan. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 9.2 : Pengurusan Capaian Pengguna • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|--|---------------------|--------------------------------|--|---|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.9.3 | Tanggungjawab pengguna Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka. | | | | | |
| | A.9.3.1 | Penggunaan maklumat pengesahan rahsia Pengguna dikehendaki mematuhi amalan organisasi dalam menggunakan maklumat pengesahan rahsia. | Peneraju ISMS (Pasukan Pusat Data & Pasukan Penilaian Pengajaran Prasiswazah di Fakulti) | YA | YA | Memastikan pengguna mengikut semua amalan yang telah ditetapkan dalam pengesahan maklumat. | <ul style="list-style-type: none"> • GPKTMK 3.0 Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) • Surat Aku Janji |
| | A.9.4 | Kawalan akses sistem dan aplikasi Menghalang akses tanpa izin kepada sistem dan aplikasi. | | | | | |
| | A.9.4.1 | Sekatan akses maklumat Akses kepada maklumat dan fungsi sistem aplikasi hendaklah dihadkan menurut dasar kawalan akses. | Peneraju ISMS | YA | YA | Memastikan akses kepada maklumat dan sistem aplikasi dihadkan mengikut prosedur kawalan akses. | <ul style="list-style-type: none"> • GPKTMK 3.0 Perkara 9.1 : Dasar Kawalan Capaian • Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) • Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) • Garis Panduan Kawalan Akses Ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|--|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | | | | | | <ul style="list-style-type: none"> Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (PU/PS/GP010/SMP-ID) Garis Panduan Pengurusan Identiti Pengguna Id eKlinik (OPR/PKU/GP13/EKLINIK-ID) Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |
| | A.9.4.2 | Prosedur log masuk yang selamat Jika dikehendaki oleh dasar kawalan akses, akses kepada sistem dan aplikasi hendaklah dikawal oleh prosedur log masuk yang selamat. | Pusat Pembangunan Maklumat dan Komunikasi & Pusat Pembangunan Akademik | YA | YA | Memastikan akses kepada sistem dan aplikasi dikawal menggunakan prosedur bersesuaian. | <ul style="list-style-type: none"> GPKTMK 3.0 Perkara 9.0 : Kawalan Akses Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) Arahan Kerja Pelaksanaan Penilaian Pengajaran (UPM/OPR/CADE/AK01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|---------|---|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | | | | | | <ul style="list-style-type: none"> Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) |
| | A.9.4.3 | Sistem pengurusan kata laluan Sistem pengurusan katalaluan hendaklah interaktif dan memastikan kata laluan yang berkualiti. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan sistem pengurusan kata laluan adalah interaktif dan kata laluan berkualiti. | <ul style="list-style-type: none"> GPCTMK 3.0 9.2 : Pengurusan Capaian Pengguna Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumt Pelajar (PU/PS/GP010/SMP-ID) Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/ UPM-ID) |
| | A.9.4.4 | Penggunaan program utiliti yang mempunyai hak istimewa Penggunaan program utiliti yang mungkin mampu melepasi kawalan sistem dan aplikasi hendaklah disekat dan dikawal dengan ketat. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan utiliti program yang boleh mengganggu sistem aplikasi perlu dihad dan dikawal. | <ul style="list-style-type: none"> GPTMK 12.2 :Perisian Berbahaya Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/PEMANTAUAN CAPAIAN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|-----------------------------|----------|--|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.9.4.5 | Kawalan akses kepada kod sumber program Akses kepada kod sumber program hendaklah dihadkan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan akses kepada program kod sumber perlu dihadkan. | <ul style="list-style-type: none"> GPKTMK 9.4 : Keselamatan Fail Sistem Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)-(iDEC/PEM/GP01) |
| A.10 KRIPTOGRAFI | A.10.1 | Kawalan kriptografi Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan/atau integriti maklumat. | | | | | |
| | A.10.1.1 | Dasar penggunaan kawalan kriptografi Dasar penggunaan kawalan kriptografi bagi melindungi maklumat hendaklah dibangunkan dan dilaksanakan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan polisi penggunaan kawalan kriptografi untuk perlindungan maklumat dibangunkan dan dilaksanakan. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian G, Klausa 21(a) GPKTMK 10.0 : Kriptografi Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|--|----------|---|---|---------------------|--------------------------------|---|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.10.1.2 | Pengurusan kekunci Dasar penggunaan, perlindungan dan tempoh hayat kekunci kriptografi hendaklah dibangunkan dan dilaksanakan sepanjang kitar hayatnya. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan polisi penggunaan, perlindungan dan jangka hayat kunci kriptografi dibangunkan dan dilaksanakan. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian G, Klausa 21(c) GPKTMK 10.0 (c) : Pengurusan <i>Public Key Infrastructure</i> (PKI) Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |
| A.11 KESELAMATAN FIZIKAL DAN PERSEKITARAN | A.11.1 | Kawasan selamat Menghalang akses fizikal tanpa kebenaran, kerosakan dan gangguan terhadap maklumat dan kemudahan pemprosesan maklumat organisasi. | | | | | |
| | A.11.1.1 | Perimeter keselamatan fizikal Perimeter keselamatan hendaklah ditakrifkan dan digunakan bagi melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat yang sensitif atau kritikal. | Peneraju ISMS | YA | YA | Memastikan perimeter keselamatan ditentukan dan digunakan untuk melindungi kawasan yang mengandungi maklumat yang sensitif atau kritikal. | <ul style="list-style-type: none"> Arahan Keselamatan : Keselamatan Fizikal Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM GPKTMK 11.1 (a) : Keselamatan Fizikal Kawasan GPKTMK 11.1(c) – Kawasan Larangan |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|----------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.1.2 | Kawalan kemasukan fizikal Kawasan selamat hendaklah dilindungi oleh kawalan kemasukan yang sesuai bagi memastikan kakitangan yang diberi kebenaran sahaja dibenarkan masuk. | Peneraju ISMS | YA | YA | Memastikan kawalan bersesuaian dilaksanakan bagi memastikan hanya pengguna yang diberi hak akses sahaja dibenarkan masuk ke dalam kawasan terkawal. | <ul style="list-style-type: none"> Arahan Keselamatan : Keselamatan Fizikal GPKTMK 11.1(b) Kawalan Masuk Fizikal Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM Prosedur Kawalan Akses (UPM/OPR/BKU/P001) Prosedur Pengoperasian Pengurusan Pusat Data (UPM/ISMS/OPR/P001) - Kawalan Akses ke Pusat Data Garis Panduan Kawalan Akses ke Pusat Data (UPM/ISMS/OPR/GP03/KAWALAN AKSES) |
| | A.11.1.3 | Keselamatan pejabat, bilik dan kemudahan Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan. | Peneraju ISMS | YA | YA | Memastikan keselamatan fizikal direka dan digunakan. | <ul style="list-style-type: none"> Arahan Keselamatan : Keselamatan Fizikal GPKTMK 11.1 (d) – Keselamatan Pejabat, Bilik dan Kemudahan Lokasi Skop Pensijilan ISMS UPM - menerusi Portal eISO UPM |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|----------------|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.1.4 | Perlindungan daripada ancaman luar dan persekitaran Perlindungan fizikal daripada bencana alam, serangan hasad atau kemalangan hendaklah direka bentuk dan dilaksanakan. | Peneraju ISMS | YA | YA | Memastikan perlindungan fizikal dibangun dan digunakan. | <ul style="list-style-type: none"> Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D, Klausa 9 (b) GPKTMK 3.0 Perkara 11.1 (e) : Kawalan Persekitaran |
| | A.11.1.5 | Bekerja di kawasan selamat Prosedur bekerja di kawasan selamat hendaklah direka bentuk dan dilaksanakan. | Peneraju ISMS | YA | YA | Memastikan prosedur bagi memastikan keselamatan tempat kerja dibangun dan dilaksanakan. | <ul style="list-style-type: none"> Akta Keselamatan dan Kesihatan Pekerjaan 1994 (AKTA 514) GPKTMK 3.0 Perkara 11.1 (f) : Bekerja dalam Kawasan Keselamatan |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.1.6 | Kawasan penyerahan dan pemunggahan Akses keluar masuk seperti kawasan penyerahan dan pemunggahan serta akses lain yang membolehkan mereka yang tidak dibenarkan melaluinya untuk memasuki premis hendaklah dikawal, dan jika boleh, diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan akses tanpa kebenaran. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawasan penghantaran dan pemunggahan perlu dikawal, jika perlu diasingkan daripada fasiliti pemprosesan maklumat bagi mengelakkan akses yang tidak dibenarkan. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D, Klausa 9 (b) GPKTMK Perkara 11.1 (g) : Kawasan Penghantaran dan Pemunggahan |
| | A.11.2 | Peralatan Untuk mengelakkan kehilangan, kerosakan, kecurian atau penjejasan aset dan gangguan terhadap operasi organisasi. | | | | | |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|----------------|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.2.1 | Penempatan dan perlindungan peralatan Peralatan hendaklah ditentukan penempatannya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran, dan peluang akses tanpa kebenaran. | Peneraju ISMS | YA | YA | Memastikan peralatan diletakkan ditempat yang dilindungi untuk mengurangkan risiko bahaya dan peluang akses yang tidak dibenarkan. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian D, Klausa 9 (b) • GKPTMK Perkara 11.3 : Keselamatan Peralatan |
| | A.11.2.2 | Utiliti sokongan Peralatan hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. | Peneraju ISMS | YA | YA | Memastikan peralatan dilindungi daripada kegagalan bekalan kuasa dan gangguan yang disebabkan oleh kegagalan utiliti sokongan. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 11.1 (h) : Perkhidmatan Sokongan • Prosedur Penyelenggaraan Berkala (UPM/SOK/PYG/P002) • Garis Panduan Penyelenggaraan Operasi Pusat Data (UPM/ISMS/OPR/GP01/ PENYELENGGARAAN OPERASI) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.2.3 | Keselamatan kabel Kabel bekalan kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kabel bekalan kuasa dan telekomunikasi dilindungi daripada pemintasan, gangguan atau kerosakan. | <ul style="list-style-type: none"> GPKTMK 3.0 Perkara 11.1 (i) : Keselamatan Kabel |
| | A.11.2.4 | Penyenggaraan peralatan Peralatan hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan integriti yang berterusan. | Peneraju ISMS | YA | YA | Memastikan peralatan diselenggara. | <ul style="list-style-type: none"> Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian D, Klausa 10 GPKTMK 3.0 Perkara 11.3 (e) : Penyelenggaraan Peralatan Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003) Perjanjian Kontrak Perkhidmatan Penyelenggaraan Manual Pelaksanaan Program Jaminan Kualiti (QAP) Dalam Perkhidmatan Radiologi Perkara 4.2 |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|--------------------------------|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.11.2.5 | Pengalihan aset Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa mendapat kebenaran terlebih dahulu. | Peneraju ISMS & Pejabat Bursar | YA | YA | Memastikan peralatan, maklumat atau perisian tidak di bawa keluar dari lokasi tanpa kebenaran. | <ul style="list-style-type: none"> GPKTMK Perkara 11.3 (f) : Peralatan di Luar Premis Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) |
| | A.11.2.6 | Keselamatan peralatan dan aset di luar premis Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis organisasi. | Peneraju ISMS & Pejabat Bursar | YA | YA | Memastikan keselamatan dan risiko setiap aset yang berada dilokasi luar diambil kira. | <ul style="list-style-type: none"> GPKTMK Perkara 11.3 (f) : Peralatan Di Luar Premis Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) |
| | A.11.2.7 | Pelupusan yang selamat atau penggunaan semula peralatan Semua bahagian peralatan yang mengandungi media penyimpanan hendaklah disahkan bagi memastikan sebarang data yang sensitif dan perisian berlesen telah | Peneraju ISMS | YA | YA | Memastikan aset yang terlibat dengan storan media perlu disemak dan data sensitif di buang sebelum diguna semula atau dimusnahkan. | <ul style="list-style-type: none"> Pekeliling Perbendaharaan Bil 5/2007 : Bab E : Pelupusan (m/s : 36) Pekeliling Bendahari Bil 1 2008 : Bahagian E Pelupusan GPKTMK 11.3 (g) : Pelupusan Peralatan Prosedur Pengurusan Aset Alih (UPM/SOK/KEW-AST/P012) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|----------------|---------------------|--------------------------------|---|---|
| Klasua | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | dikeluarkan atau berjaya ditulis ganti sebelum dilupuskan atau diguna semula. | | | | | |
| | A.11.2.8 | Peralatan pengguna tanpa jagaan Pengguna hendaklah memastikan peralatan yang dibiarkan tanpa jagaan mempunyai perlindungan sewajarnya. | Peneraju ISMS | YA | YA | Memastikan peralatan yang ditinggalkan di kawal dengan dengan sempurna. | <ul style="list-style-type: none"> GPKTMK Perkara 11.3 (h) : Peralatan Ditinggalkan Pengguna |
| | A.11.2.9 | Dasar meja bersih dan skrin kosong Dasar meja bersih untuk pengendalian kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. | Peneraju ISMS | YA | YA | Memastikan polisi <i>clear desk</i> dan <i>clear screen</i> diguna pakai. | <ul style="list-style-type: none"> GPKTMK Perkara 11.3 (i) : Panduan <i>Clear Desk</i> dan <i>Clear Screen</i> Buku Panduan Perkhidmatan Perubatan Pusat Kesihatan Universiti |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|-------------------------------------|----------|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.12 KESELAMATAN OPERASI | A.12.1 | Prosedur dan tanggungjawab operasi Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat. | | | | | |
| | A.12.1.1 | Prosedur operasi yang didokumenkan Prosedur operasi hendaklah didokumenkan dan disediakan untuk semua pengguna yang memerlukannya. | Pusat Jaminan Kualiti | YA | YA | Memastikan prosedur operasi didokumen dan disediakan kepada yang memerlukan. | <ul style="list-style-type: none"> Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) Sistem Pengurusan ISO UPM (e-ISO) - http://reg.upm.edu.my/eISO |
| | A.12.1.2 | Pengurusan perubahan Perubahan dalam organisasi, proses perniagaan, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. | Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan perubahan kepada organisasi, proses bisnes dan fasiliti pemprosesan maklumat dikawal. | <ul style="list-style-type: none"> Bidang kuasa Pihak Berkuasa Universiti di bawah Seksyen 16 Perlembagaan UPM termasuklah: <ol style="list-style-type: none"> Bidang kuasa Lembaga Pengarah Universiti Bidang kuasa Senat Universiti Bidang kuasa Jawatankuasa Tetap Kewangan Bidang kuasa Jawatankuasa Pengurusan Universiti Bidang kuasa Mesyuarat Kajian Semula Pengurusan Bidang kuasa Jawatankuasa Kualiti |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | | | | | | <ul style="list-style-type: none"> Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) |
| | A.12.1.3 | Pengurusan kapasiti Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan kapasiti masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. | Peneraju ISMS | YA | YA | Memastikan penggunaan sumber dipantau dan unjuran dibuat untuk keperluan masa depan untuk memastikan keperluan prestasi sistem. | <ul style="list-style-type: none"> GPKTMK 12.1 (d): Pengurusan Kapasiti Prosedur Penyelenggaraan ICT (UPM/OPR/IDEC/P003) Arahan Kerja Konfigurasi Server (UPM/ISMS/OPR/AK11) |
| | A.12.1.4 | Pengasingan persekitaran pembangunan, pengujian dan operasi Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko akses tanpa izin atau perubahan | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pembangunan, pengujian dan operasi persekitaran diasingkan untuk mengurangkan risiko kepada akses yang tidak dibenarkan. | <ul style="list-style-type: none"> GPKTMK 14.3(a) : Prosedur Kawalan Persekitaran Selamat Garis Panduan Penyediaan Server Di Pusat Data (UPM/ISMS/OPR/GP02/PENYEDIAAN SERVER) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | kepada persekitaran operasi. | | | | | |
| | A.12.2 | Perlindungan daripada perisian hasad Memastikan maklumat dan kemudahan pemprosesan maklumat dilindungi daripada perisian hasad. | | | | | |
| | A.12.2.1 | Kawalan daripada perisian hasad Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada perisian hasad hendaklah dilaksanakan, digabungkan dengan kesedaran pengguna yang sewajarnya. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawalan ke atas perisian hasad (<i>malware</i>) dibangunkan. | <ul style="list-style-type: none"> GPKTMK 12.2 (a) : Perlindungan daripada Perisian Berbahaya |
| | A.12.3 | Sandaran Melindungi kehilangan data. | | | | | |
| | A.12.3.1 | Sandaran maklumat Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut dasar sandaran yang dipersetujui. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan salinan pendua dilaksanakan dan diuji secara berkala. | <ul style="list-style-type: none"> GPKTMK Perkara 12.3 (a) : <i>Backup</i> Garis Panduan Pengurusan <i>Backup</i> Pangkalan Data dan Aplikasi (UPM/ISMS/OPR/GP14/BACKUP) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|--|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.12.4 | Pengelogan dan pemantauan Merekodkan kejadian dan menghasilkan bukti. | | | | | |
| | A.12.4.1 | Pengelogan kejadian Log kejadian yang merekodkan aktiviti pengguna, pengecualian, ralat dan kejadian keselamatan maklumat hendaklah dihasilkan, disimpan dan dikaji semula secara tetap. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan <i>event log</i> dijana, disimpan dan dikaji secara berkala. | <ul style="list-style-type: none"> GPKTMK 12.4: <i>Logging</i> dan Pemantauan |
| | A.12.4.2 | Perlindungan maklumat log Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan akses tanpa izin. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kemudahan dan maklumat dilindungi daripada akses yang tidak dibenarkan. | <ul style="list-style-type: none"> GPKTMK 12.4 (b): Perlindungan Maklumat Log Garis Panduan Pemantauan Capaian Ke Sistem (UPM/ISMS/OPR/GP06/Pemantauan Capaian) |
| | A.12.4.3 | Log pentadbir dan pengendali Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log tersebut hendaklah | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan aktiviti pentadbir sistem direkod, dikawal dan di pantau berkala. | <ul style="list-style-type: none"> GPKTMK 12.4 (c): Pentadbir dan Operator Log Prosedur Kawalan dan Pemantauan Capaian ke Sistem di Pusat Data (UPM/ISMS/OPR/P003) Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07/IDENTITI) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|---|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | dilindungi dan dikaji semula secara tetap. | | | | | <ul style="list-style-type: none"> Garis Panduan Perlindungan Maklumat Log Server (UPM/ISMS/OPR/GP08/MAKLUMAT LOG) |
| | A.12.4.4 | Penyegerakkan jam Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah disegerakkan mengikut satu sumber rujukan masa. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan masa bagi semua pemprosesan maklumat diselaraskan dengan satu sumber rujukan masa. | <ul style="list-style-type: none"> GPCTMK12.4 (d): Pelarasan Masa <i>Network Time Protocol</i> (time.upm.edu.my) |
| | A.12.5 | Kawalan perisian yang beroperasi Memastikan kewibawaan sistem yang beroperasi. | | | | | |
| | A.12.5.1 | Pemasangan perisian pada sistem yang beroperasi Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang beroperasi. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawalan pemasangan perisian ke atas sistem pengoperasian. | <ul style="list-style-type: none"> GPCTMK 12.5: Kawalan Ke atas Perisian Pengoperasian Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) Panduan Instalasi Sistem yang berkaitan |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.12.6 | Pengurusan kerentanan teknikal Mencegah eksploitasi kerentanan teknikal. | | | | | |
| | A.12.6.1 | Pengurusan kerentanan teknikal Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan maklumat berkaitan kelemahan terhadap sistem dinilai dan diukur. | <ul style="list-style-type: none"> • GKPTMK 12.6: Pengurusan Kerentanan Teknikal • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/ /GP09/TAHAP KESELAMATAN) • Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|---|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.12.6.2 | Sekatan ke atas pemasangan perisian Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan peraturan kawalan instalasi perisian dibangun dan dilaksanakan. | <ul style="list-style-type: none"> GPKTMK 12.6 (b): Menghadkan Instalasi Perisian Panduan Instalasi Sistem yang berkaitan |
| | A.12.7 | Pertimbangan tentang audit sistem maklumat Meminimumkan kesan aktiviti audit ke atas sistem yang beroperasi. | | | | | |
| | A.12.7.1 | Kawalan audit sistem maklumat Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan. | Pusat Jaminan Kualiti & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan keperluan audit dan aktiviti yang melibatkan pengesahan terhadap sistem operasi dirancang dengan teliti dan dipersetujui untuk meminimumkan gangguan (disruption) pada proses sesebuah organisasi. | <ul style="list-style-type: none"> GPKTMK 12.7: Kawalan Audit Sistem Maklumat Audit Dalaman ISMS |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|--|----------|--|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.13 KESELAMATAN KOMUNIKASI | A.13.1 | Pengurusan keselamatan rangkaian Memastikan perlindungan maklumat dalam rangkaian dan dalam kemudahan sokongan pemprosesan maklumat dalam rangkaian. | | | | | |
| | A.13.1.1 | Kawalan rangkaian Rangkaian hendaklah diurus dan dikawal bagi melindungi maklumat dalam sistem dan aplikasi. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan rangkaian perlu urus dan dikawal. | <ul style="list-style-type: none"> • GKPTMK 13.1 : Pengurusan Keselamatan Rangkaian • GKPTMK 13.2 : Kawalan Akses Rangkaian • Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR/ /GP13/AGIHAN RANGKAIAN) • Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/GP16/UPM-ID) |
| | A.13.1.2 | Keselamatan perkhidmatan rangkaian Mekanisme keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian, sama ada | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Tidak melibatkan <i>Internet service provider</i> . Hanya menggunakan intranet (UPMNET). | <ul style="list-style-type: none"> • GKPTMK 13.1 Pengurusan Keselamatan Rangkaian • Kontrak Perkhidmatan Internet antara UPM dengan <i>Network Service Provider</i> (NSP) • Kontrak perkhidmatan <i>Firewall</i> dan WAF dengan pembekal |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|-----|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | perkhidmatan ini disediakan secara dalaman atau oleh khidmat luaran. | | | | | |
| A.13.1.3 | | Pengasingan dalam rangkaian Kelompok perkhidmatan maklumat, pengguna dan sistem maklumat hendaklah diasingkan dalam rangkaian. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pengasingan rangkaian dilaksanakan. | <ul style="list-style-type: none"> Garis Panduan Pengurusan Pengagihan Rangkaian (UPM/ISMS/OPR /GP13/AGIHAN RANGKAIAN) |
| A.13.2 | | Pemindahan maklumat Memelihara keselamatan maklumat yang dipindahkan dalam sesebuah organisasi dan dengan mana-mana entiti luaran. | | | | | |
| A.13.2.1 | | Dasar dan prosedur pemindahan maklumat Dasar, prosedur dan kawalan pemindahan formal hendaklah disediakan bagi melindungi pemindahan maklumat melalui penggunaan semua jenis kemudahan komunikasi. | Peneraju ISMS | YA | YA | Memastikan polisi dan kawalan terhadap pemindahan maklumat perlu disediakan. | <ul style="list-style-type: none"> GPKTMK 13.3 : Pengurusan Pertukaran Maklumat Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|--|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.13.2.2 | Perjanjian tentang pemindahan maklumat Perjanjian hendaklah menangani aspek keselamatan dalam pemindahan maklumat perniagaan antara organisasi dengan pihak luaran. | Peneraju ISMS & Pejabat Bursar | YA | YA | Memastikan kontrak perjanjian memenuhi keperluan keselamatan penghantaran maklumat diantara pembekal dan organisasi. | <ul style="list-style-type: none"> • GKPTMK 13.3(a) : Pertukaran Maklumat • Peraturan Kewangan • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) |
| | A.13.2.3 | Pesanan elektronik Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya. | Pusat Pembangunan Maklumat dan Komunikasi, Pejabat Pendaftar & Pusat Strategi dan Perhubungan Korporat | YA | YA | Memastikan kawalan terhadap pesanan elektronik dibangunkan. | <ul style="list-style-type: none"> • Akta Rahsia Rasmi 1972 • Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F • GKPTMK Perkara 13.3 (b): Pengurusan Mel Elektronik • Garis Panduan E-mel UPM • Panduan Amalan Komunikasi Berkesan • Surat Aku Janji |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|---|----------|---|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.13.2.4 | Perjanjian kerahsiaan atau ketakdedahan Keperluan untuk perjanjian kerahsiaan atau ketakdedahan yang menggambarkan keperluan organisasi terhadap perlindungan maklumat hendaklah dikenal pasti, dikaji semula dan didokumenkan secara tetap. | Pejabat Pendaftar & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan NDA bagi keperluan melindungi maklumat perlu dikenal pasti, di pantau dan didokumenkan. | <ul style="list-style-type: none"> Akta Rahsia Rasmi 1972 Akta Arkib Negara 2003 (Akta 629) GPKTMK Perkara 15.1 : Pihak Ketiga Borang Permohonan Data (OPR/PEND/BRO1/DATA). Bahagian D:Perakuan Pemohon dan Pengesahan Ketua PTJ/Ketua Jabatan untuk Sokongan <i>Non Discloser Agreement (NDA)</i> Surat Aku Janji Surat Aku Janji Pihak Luar |
| A.14 PENEROLEHAN, PEMBANGUNAN DAN PENYENGKARAAN SISTEM | A.14.1 | Keperluan keselamatan sistem maklumat Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan melalui rangkaian awam. | | | | | |
| | A.14.1.1 | Analisis dan spesifikasi keperluan keselamatan maklumat Keperluan berkaitan keselamatan maklumat hendaklah disertakan dalam keperluan untuk | Peneraju ISMS | YA | YA | Memastikan keperluan keselamatan maklumat perlu dimasukkan ke dalam sistem baharu atau sistem sedia ada. | <ul style="list-style-type: none"> Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)-(iDEC/PEM/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|--|--|
| Klasa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. | | | | | |
| | A.14.1.2 | Melindungi perkhidmatan aplikasi dalam rangkaian awam Maklumat yang terlibat dalam perkhidmatan aplikasi yang disebarkan melalui rangkaian awam hendaklah dilindungi daripada aktiviti pemalsuan, pertikaian kontrak serta pendedahan dan pengubahsuaian yang tidak dibenarkan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawalan terhadap rangkaian awam perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan atau pengubahsuaian yang tidak dibenarkan. | <ul style="list-style-type: none"> GPTMK 3.0 Perkara 13.1 : Pengurusan Keselamatan Rangkaian Garis Panduan Keselamatan Peralatan Mudah Alih (UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH) 2.0 Panduan 1(viii) Perlaksanaan <i>Network Authentication</i> UPM https://authenticate.upm.edu.my/ |
| | A.14.1.3 | Melindungi transaksi perkhidmatan aplikasi Maklumat yang terlibat dalam transaksi perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan maklumat yang terlibat dalam transaksi perkhidmatan aplikasi dilindungi untuk menghalang penghantaran yang tidak lengkap, tersalah laluan , | <ul style="list-style-type: none"> GPTMK 14.1 (c) – Melindungi Transaksi Perkhidmatan Aplikasi Perlaksanaan <i>Secure Socket Layer-SSL</i> di Sistem Aplikasi |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|-----|---|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | tidak sempurna, salah hala, pindaan mesej tanpa kebenaran, pendedahan tanpa kebenaran, duplikasi atau ulang tayang mesej tanpa kebenaran. | | | | pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, duplikasi mesej yang tidak dibenarkan atau ulangan. | |
| A.14.2 | | Keselamatan dalam proses pembangunan dan sokongan Memastikan keselamatan maklumat direka bentuk dan dilaksanakan dalam kitar hayat pembangunan sistem maklumat. | | | | | |
| A.14.2.1 | | Dasar pembangunan selamat Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan polisi keselamatan pembangunan sistem dan aplikasi dibangun dan diguna pakai. | <ul style="list-style-type: none"> • GKPTMK Perkara 14.1 : Keselamatan dalam Pembangunan Sistem dan Aplikasi • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi) (iDEC/PEM/GP01) |
| A.14.2.2 | | Prosedur kawalan perubahan sistem Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan perubahan kepada proses pembangunan perlu dikawal menggunakan prosedur kawalan perubahan. | <ul style="list-style-type: none"> • GKPTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | menggunakan prosedur kawalan perubahan formal. | | | | | |
| | A.14.2.3 | Kajian semula teknikal bagi aplikasi selepas perubahan platform operasi Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada impak yang menjejaskan ke atas operasi atau keselamatan organisasi. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan perubahan ke atas aplikasi perlu di semak dan diuji untuk memastikan tiada kesan buruk terhadap organisasi atau keselamatan. | <ul style="list-style-type: none"> • GKPTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) |
| | A.14.2.4 | Sekatan ke atas perubahan dalam pakej perisian Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan sebarang perubahan atau pengubahsuaian pakej aplikasi perlu dikawal. | <ul style="list-style-type: none"> • GKPTMK Perkara 14.2 (a) : Prosedur Kawalan Perubahan • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.14.2.5 | Prinsip kejuruteraan sistem yang selamat Prinsip kejuruteraan bagi sistem yang selamat hendaklah diwujudkan, didokumenkan, disenggara dan digunakan untuk sebarang usaha pelaksanaan sistem maklumat. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan prinsip persekitaran pembangunan selamat diamalkan dalam setiap projek pembangunan sistem aplikasi. | <ul style="list-style-type: none"> • GKPTMK 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)-(iDEC/PEM/GP01) |
| | A.14.2.6 | Persekitaran pembangunan selamat Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan persekitaran pembangunan selamat diamalkan dalam setiap proses pembangunan sistem aplikasi. | <ul style="list-style-type: none"> • GKPTMK 3.0 Perkara 14.3 : Persekitaran Pembangunan Selamat • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi (OPR/iDEC/GP06/Pengaturcaraan Aplikasi)-(iDEC/PEM/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.14.2.7 | Pembangunan oleh khidmat luaran Organisasi hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dijalankan oleh khidmat luaran. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan aktiviti pembangunan oleh pihak luar perlu diselia dan dipantau. | <ul style="list-style-type: none"> • GPKTMK 14.3 (C) : Pembangunan Sistem Aplikasi oleh Pihak Ketiga • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Dokumen Kontrak |
| | A.14.2.8 | Pengujian keselamatan sistem Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan ujian keselamatan perlu dilaksanakan semasa pembangunan aplikasi. | <ul style="list-style-type: none"> • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/TAHAP KESELAMATAN) |
| | A.14.2.9 | Pengujian penerimaan sistem Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan ujian penerimaan perlu dilaksanakan bagi sistem baru atau naik taraf. | <ul style="list-style-type: none"> • Prosedur Pembangunan ICT (UPM/OPR/IDEC/P001) • Garis Panduan Pelaksanaan Pengujian Sistem Aplikasi (OPR/IDEC/GP05/Pengujian Aplikasi) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|-----------------------------------|----------|---|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.14.3 | Data ujian Memastikan perlindungan bagi data yang digunakan untuk pengujian. | | | | | |
| | A.14.3.1 | Perlindungan data ujian Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan data pengujian dipilih, dilindungi dan dikawal. | <ul style="list-style-type: none"> • GPKTMK Perkara 14.3 (b. iii) : Pengujian Pembangunan atau Penaiktarafan Sistem • Arahan Kerja Perkhidmatan Sokongan ICT (UPM/OPR/IDEC/AK31 Perkhidmatan Sokongan ICT) - 3.3.2 Pengurusan Data dan Implimentasi |
| A.15 HUBUNGAN PEMBEKAL | A.15.1 | Keselamatan maklumat dalam hubungan pembekal Memastikan perlindungan aset organisasi yang boleh diakses oleh pembekal. | | | | | |
| | A.15.1.1 | Dasar keselamatan maklumat untuk hubungan pembekal Keperluan keselamatan maklumat untuk mengurangkan risiko yang dikaitkan dengan akses pembekal kepada aset organisasi hendaklah dipersetujui dengan | Peneraju ISMS | YA | YA | Memastikan keperluan keselamatan maklumat didokumenkan dan dipersetujui oleh pihak pembekal. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F, Klausa 16 (c) • GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Surat Aku Janji Pihak Luar • Kontrak Bekalan/Perkhidmatan |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|----------------|---------------------|--------------------------------|---|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | pembekal dan didokumenkan. | | | | | |
| | A.15.1.2 | Menangani keselamatan dalam perjanjian pembekal Semua keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur IT untuk maklumat organisasi. | Peneraju ISMS | YA | YA | Memastikan keperluan keselamatan maklumat dibangunkan dan dipersetujui oleh pihak pembekal. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian F, Klausa 16 (c) • GPKTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Dokumen Perjanjian antara UPM dan Pihak Pembekal • Surat Aku Janji Pihak Luar • Kontrak Bekalan/Perkhidmatan |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|--|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.15.1.3 | Rantaian bekalan teknologi maklumat dan komunikasi Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk menangani risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. | Pejabat Bursar & Pejabat Penasihat Undang-Undang | YA | YA | Memastikan dokumen perjanjian antara pihak pembekal memenuhi keperluan keselamatan maklumat. | <ul style="list-style-type: none"> • GKPTMK Perkara 15.1 : Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) • Senarai Semak Surat Cara Undang-undang (Perjanjian/Persefahaman) |
| | A.15.2 | Pengurusan penyampaian perkhidmatan pembekal Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal. | | | | | |
| | A.15.2.1 | Memantau dan mengkaji semula perkhidmatan pembekal Organisasi hendaklah memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal secara tetap. | Pejabat Bursar | YA | YA | Memastikan pemantauan, semakan terhadap penerimaan perkhidmatan pembekal dijalankan secara berkala. | <ul style="list-style-type: none"> • GKPTMK Perkara 15.2 : Pengurusan Penyampaian Perkhidmatan Pihak Ketiga • Arahan Kerja Penilaian Prestasi Syarikat (UPM/SOK/KEW/AK002/BUY) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|--|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.15.2.2 | Menguruskan perubahan kepada perkhidmatan pembekal Perubahan kepada perolehan perkhidmatan daripada pembekal, termasuk mengekalkan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan pentaksiran semula risiko. | Pejabat Bursar & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan polisi, prosedur dan kawalan bagi mengurus perubahan penyediaan perkhidmatan dilaksanakan. | <ul style="list-style-type: none"> • GKPTMK Perkara 15.2 : Pengurusan Penyampaian Perkhidmatan Pihak Ketiga • Prosedur Perolehan Universiti (UPM/SOK/KEW-BUY/P016) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|---|----------|---|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.16 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT | A.16.1 | Pengurusan insiden keselamatan maklumat dan penambahbaikan Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kelemahan keselamatan. | | | | | |
| | A.16.1.1 | Tanggungjawab dan prosedur Tanggungjawab pengurusan dan prosedur hendaklah diwujudkan bagi memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan prosedur dan tanggungjawab pengurusan dibangunkan untuk memastikan tindak balas yang cepat dan berkesan terhadap insiden keselamatan. | <ul style="list-style-type: none"> Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |
| | A.16.1.2 | Pelaporan kejadian keselamatan maklumat Kejadian keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang bersesuaian dengan secepat mungkin. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan insiden keselamatan dilapor dengan cepat melalui saluran pengurusan yang betul. | <ul style="list-style-type: none"> Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.16.1.3 | Pelaporan kelemahan keselamatan maklumat Kakitangan dan kontraktor yang menggunakan sistem dan perkhidmatan maklumat organisasi adalah dikehendaki mencatatkan dan melaporkan sebarang kelemahan keselamatan maklumat yang diperhatikan atau disyaki dalam sistem atau perkhidmatan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pekerja dan pembekal melaporkan kelemahan keselamatan yang terdapat pada sistem atau perkhidmatan. | <ul style="list-style-type: none"> • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |
| | A.16.1.4 | Penilaian dan keputusan tentang kejadian keselamatan maklumat Kejadian keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan insiden keselamatan dinilai dan diputuskan sekiranya diklasifikasikan sebagai insiden keselamatan maklumat. | <ul style="list-style-type: none"> • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|---|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.16.1.5 | Tindak balas terhadap insiden keselamatan maklumat Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pengurusan insiden keselamatan mengikut prosedur. | <ul style="list-style-type: none"> • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Prosedur Perkhidmatan ICT (UPM/OPR/IDEC/P002) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |
| | A.16.1.6 | Mempelajari daripada insiden keselamatan maklumat Pengetahuan yang diperoleh daripada analisis dan penyelesaian insiden keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya insiden atau impak insiden mendatang. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan analisis dan penyelesaian terhadap insiden keselamatan berlaku boleh digunakan untuk mengurangkan kemungkinan atau kesan pada masa akan datang. | <ul style="list-style-type: none"> • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.16.1.7 | Pengumpulan bahan bukti Organisasi hendaklah mentakrifkan dan menggunakan prosedur untuk mengenal pasti, mengumpul, memperoleh dan memelihara maklumat yang boleh digunakan sebagai bahan bukti. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan pengenalpastian, pengumpulan dan pemuliharaan maklumat perlu dilaksanakan sebagai bukti tindakan. | <ul style="list-style-type: none"> • GKPTMK 12.4: <i>Logging</i> dan Pemantauan • Pelan pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|--|----------|--|--|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| A.17 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERNIAGAAN | A.17.1 | Kesinambungan keselamatan maklumat Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perniagaan organisasi. | | | | | |
| | A.17.1.1 | Perancangan kesinambungan keselamatan maklumat Organisasi hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam keadaan yang menjejaskan, contohnya, semasa krisis atau bencana. | Pejabat Pengurusan Keselamatan dan Kesihatan Pekerja & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan keperluan kesinambungan pengurusan keselamatan maklumat. | <ul style="list-style-type: none"> • GKPTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) |
| | A.17.1.2 | Pelaksanaan kesinambungan keselamatan maklumat Organisasi hendaklah mewujudkan, mendokumenkan, melaksanakan dan menyenggarakan proses, | Pejabat Pengurusan Keselamatan dan Kesihatan Pekerja & Pusat Pembangunan | YA | YA | Memastikan prosedur dan kawalan bagi kesinambungan perkhidmatan dibangun dan didokumenkan. | <ul style="list-style-type: none"> • GKPTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|--|---------------------|--------------------------------|--|--|
| Klasua | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. | Maklumat dan Komunikasi | | | | |
| | A.17.1.3 | Menentusahkan, mengkaji semula dan menilai kesinambungan keselamatan maklumat Organisasi hendaklah menentusahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikan ianya sah dan berkesan semasa keadaan yang menjejaskan. | Pejabat Pengurusan Keselamatan dan Kesihatan Pekerja & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan maklumat kawalan kesinambungan keselamatan disahkan dan dilaksanakan secara berkala untuk memastikan ia berkesan sekiranya berlaku bencana. | <ul style="list-style-type: none"> • GKPTMK 17.0 – Pengurusan Kesinambungan Perkhidmatan • Pelan Kesinambungan Perkhidmatan • Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) • Laporan Pengujian Simulasi DRP ICT UPM |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|---|--|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.17.2 | Lewahan Memastikan ketersediaan kemudahan pemprosesan maklumat. | | | | | |
| | A.17.2.1 | Ketersediaan kemudahan pemprosesan maklumat Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan lewahan yang mencukupi bagi memenuhi keperluan ketersediaan. | Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi, | YA | YA | Memastikan fasiliti pemprosesan dibangunkan bagi memenuhi keperluan ketersediaan maklumat. | <ul style="list-style-type: none"> Pelan Kesenambungan Perkhidmatan Pelan Pemulihan Bencana ICT Universiti Putra Malaysia (DRP ICT) |
| A.18 PEMATUHAN | A.18.1 | Pematuhan kepada keperluan undang-undang dan kontrak Mengelakkan pelanggaran obligasi undang-undang, statutori, kawal selia atau kontrak yang berkaitan dengan keselamatan maklumat dan sebarang keperluan keselamatan. | | | | | |
| | A.18.1.1 | Pengenalpastian keperluan undang-undang dan kontrak yang terpakai Semua keperluan perundangan, statutori, kawal selia, kontrak yang berkaitan dan pendekatan organisasi bagi memenuhi keperluan ini hendaklah dikenal pasti dengan jelas, | Pejabat Penasihat Undang-undang | YA | YA | Memastikan keperluan perundangan dikenal pasti dan didokumenkan serta dikemaskini. | <ul style="list-style-type: none"> GPKTMK Perkara 18.1 (d) : Keperluan Perundangan Senarai Undang-undang sedia ada melalui Portal eISO |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | | didokumenkan dan dikemas kini bagi setiap sistem maklumat dan organisasi. | | | | | |
| | A.18.1.2 | Hak harta intelek Prosedur yang sesuai hendaklah dilaksanakan bagi memastikan keperluan pematuhan perundangan, kawal selia dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk perisian proprietari. | Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan prosedur bersesuaian dibangunkan untuk memastikan pematuhan kepada undang-undang. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan komunikasi) 2014, Bahagian D, Klausa 12 • Jawatankuasa Teknologi Maklumat dan Komunikasi UPM • Kontrak Bekalan/Perkhidmatan |
| | A.18.1.3 | Perlindungan rekod Rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan pengeluaran tanpa kebenaran, mengikut keperluan undang-undang, kawal selia, kontrak dan perniagaan. | Peneraju ISMS | YA | YA | Memastikan rekod perlu di lindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran, peraturan, kontra atau keperluan bisnes. | <ul style="list-style-type: none"> • Akta Arkib Negara 2003 (Akta 629) • GPKTMK Perkara 8.3 (c) : Keselamatan Dokumen • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Garis Panduan Pengurusan Keselamatan Perlindungan Dokumen Rasmi Universiti Putra Malaysia • Panduan Pengurusan Fail dan Rekod Universiti |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|---|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.18.1.4 | Privasi dan perlindungan maklumat peribadi Privasi dan perlindungan maklumat peribadi hendaklah dipastikan seperti yang dikehendaki dalam undang-undang dan peraturan yang relevan jika berkenaan. | Peneraju ISMS & Pejabat Pendaftar | YA | YA | Memastikan perlindungan terhadap maklumat peribadi memenuhi keperluan perundangan berkaitan. | <ul style="list-style-type: none"> • GPKTMK Perkara 13.3 : Pengurusan Pertukaran Maklumat • Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) • Prosedur Pertukaran Maklumat (UPM/ISMS/SOK/P002) • Borang Pergerakan Fail Pejabat Pendaftar (Fail Peribadi) |
| | A.18.1.5 | Peraturan kawalan kriptografi Kawalan kriptografi hendaklah digunakan bagi mematuhi semua perjanjian, undang-undang dan peraturan yang relevan. | Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan kawalan kriptografi digunakan dengan mematuhi semua perjanjian berkenaan, undang-undang dan peraturan. | <ul style="list-style-type: none"> • Kaedah-kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014, Bahagian G, Klausa 21 • GPKTMK Perkara 10.0 : Kawalan Kriptografi • Garis Panduan Pengendalian Maklumat (iDEC/ISMS/GP01) |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|-----------------------|---------------------|--------------------------------|--|---|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.18.2 | Kajian semula keselamatan maklumat Memastikan keselamatan maklumat dilaksanakan dan dikendalikan menurut dasar dan prosedur organisasi. | | | | | |
| | A.18.2.1 | Kajian semula keselamatan maklumat secara berkecuali Pendekatan organisasi dalam menguruskan keselamatan maklumat dan pelaksanaannya (iaitu, objektif kawalan, kawalan, dasar, proses dan prosedur untuk keselamatan maklumat) hendaklah dikaji semula secara berkecuali pada sela masa yang dirancang atau apabila berlaku perubahan yang ketara. | Pusat Jaminan Kualiti | YA | YA | Memastikan pengurusan keselamatan maklumat dikaji semula secara berkala atau apabila perubahan ketara berlaku. | <ul style="list-style-type: none"> Mesyuarat Kajian Semula Pengurusan UPM Mesyuarat Jawatankuasa Kualiti UPM Mesyuarat Jawatankuasa Kerja ISMS |



**PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT**

| Kawalan ISO/IEC 27001:2013 | | | Pemilik Proses | Terpakai (Ya/Tidak) | Dilaksanakan (Ya/Separa/Tidak) | Justifikasi | Kawalan Semasa |
|----------------------------|----------|--|---|---------------------|--------------------------------|--|--|
| Klausa | Sek | Objektif Kawalan/ Kawalan | | | | | |
| | A.18.2.2 | Pematuhan dasar dan standard keselamatan Pengurus hendaklah mengkaji semula secara tetap pemuatnahan pemprosesan maklumat dan prosedur dalam bidang tanggungjawabnya terhadap dasar keselamatan yang bersesuaian, standard dan sebarang keperluan keselamatan yang lain. | Pusat Jaminan Kualiti | YA | YA | Memastikan pemuatnahan ke atas proses dan prosedur disemak semula dengan dasar-dasar keselamatan yang sesuai, standard dan sebarang keperluan keselamatan yang lain. | <ul style="list-style-type: none"> Prosedur Pengurusan Dokumen ISO (UPM/PGR/P001) Mesyuarat Jawatankuasa Kualiti UPM |
| | A.18.2.3 | Kajian semula pemuatnahan teknikal Sistem maklumat hendaklah dikaji semula secara tetap bagi mematuhi dasar dan standard keselamatan maklumat organisasi. | Peneraju ISMS & Pusat Pembangunan Maklumat dan Komunikasi | YA | YA | Memastikan sistem maklumat hendaklah dikaji semula secara berkala untuk mematuhi dasar dan standard keselamatan maklumat organisasi. | <ul style="list-style-type: none"> Mesyuarat Jawatankuasa Keselamatan Teknologi Maklumat & Komunikasi UPMCert Garis Panduan Penilaian Tahap Keselamatan (UPM/ISMS/OPR/GP09/Tahap Keselamatan) |

Nota: terma 'staf' ditukar kepada 'pekerja' selaras dengan penggunaan terma tersebut dalam Dasar Kualiti yang diluluskan oleh Lembaga Pengurusan Universiti pada 10 Disember 2019. Pengemaskinian ke atas dokumen terkawal dan dokumen rujukan lain yang terlibat dalam proses kerja akan dibuat secara berperingkat.

DOKUMEN RUJUKAN PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT



ISO/IEC 27001

DOKUMEN RUJUKAN PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT UPM

Senarai Kandungan

| <u>Bil.</u> | <u>Perkara</u> | <u>Muka surat</u> |
|-------------|---|-------------------|
| 1. | Pengenalan | |
| 1.1 | Pengenalan ISMS | 3 |
| 1.2 | Sejarah Pelaksanaan ISMS di UPM | 3 |
| 2. | PELAKSANAAN ISMS | |
| 2.1 | Dasar ISMS | 4 |
| 2.2 | Skop Pensijilan, Pengecualian Skop dan Pusat Tanggungjawab (PTJ) yang Terlibat | 4 |
| 2.3 | Objektif ISMS | 4 |
| 2.4 | Pihak Berkepentingan dan Keperluan Mereka | 4 |
| 2.5 | Isu Dalaman dan Isu Luaran | 5 |
| 2.6 | Pengurusan Risiko | 5 |
| 3. | PENYATA PEMAKAIAN [<i>STATEMENT OF APPLICABILITY (SOA)</i>] | 6 |
| 4. | JAWATANKUASA DAN PERANAN | |
| 4.1 | Struktur Organisasi ISMS | 6 |
| 4.2 | Peranan dan Tanggungjawab | 6 |
| 5. | SENARAI <i>STANDARD OPERATION PROCEDURE (SOP)</i> YANG DIRUJUK | 7 |

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 Klausula 4: Konteks Organisasi hingga Klausula 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 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. Alhamdulillah UPM telah berjaya melepasi peringkat persijilan ini dan 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. Sejar dengan itu juga, no. Pensijilan ISMS telah dipinda kepada ISMS 00150 berdasarkan ketetapan terkini oleh pihak SIRIM.

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; 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 dan aktiviti kemasukan pendaftaran pelajar baharu prasiswazah untuk:

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

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 Dalam dan Isu Luaran

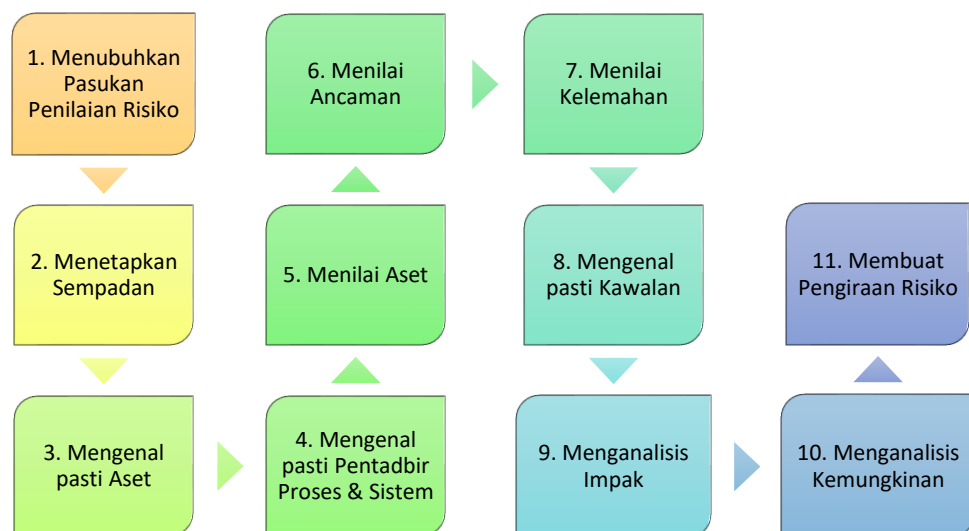
Isu dalaman dan isu luaran yang terlibat dengan pelaksanaan Sistem Pengurusan Keselamatan Maklumat UPM adalah sebagaimana paparan dalam Sistem Pengurusan ISO (eISO) UPM (<http://reg.upm.edu.my/eISO>).

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. | 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/KEW-BUY/P016 | Prosedur Perolehan Universiti | Pejabat Bursar |
| 8. | UPM/SOK/KEW-AST/P012 | Prosedur Pengurusan Aset Alih | Pejabat Bursar |
| 9. | UPM/SOK/KEW/GP020/AST | Garis Panduan Pelupusan Aset Alih | Pejabat Bursar |
| 10. | UPM/SOK/KEW/AK002/BUY | Arahan Kerja Penilaian Prestasi Syarikat | Pejabat Bursar |
| 11. | UPM/SOK/LAT/P001 | Prosedur Pengurusan Latihan Pekerja Universiti Putra Malaysia | Pejabat Pendaftar |
| 12. | UPM/OPR/PNC-UI/P001 UPM/OPR/PEND/P016 | Prosedur Pengurusan Mesyuarat Tatatertib Staf Pekerja | Unit Integriti, Pejabat Naib Pejabat Pendaftar |
| 13. | UPM/OPR/BUR-BUY/P003 | Prosedur Pendaftaran Syarikat dan Pekerja/Individu | Pejabat Bursar |
| 14. | UPM/OPR/iDEC/P001 | Prosedur Pembangunan ICT | Pusat Pembangunan Maklumat dan Komunikasi |
| 15. | UPM/OPR/iDEC/P002 | Prosedur Perkhidmatan ICT | Pusat Pembangunan Maklumat dan Komunikasi |
| 16. | UPM/OPR/iDEC/P003 | Prosedur Penyelenggaraan ICT | Pusat Pembangunan Maklumat dan Komunikasi |

| SOP QMS YANG DIRUJUK DALAM PELAKSANAAN ISMS DI UPM | | | |
|--|---|---|--|
| Bil | Kod Dokumen | Nama Dokumen | Peneraju Proses |
| 17. | UPM/OPR/CADE/AK01 | Arahan Kerja Pelaksanaan Penilaian Pengajaran | Pusat Pembangunan Akademik |
| 18. | OPR/iDEC/GP06/ PENGATURCARAAN APLIKASI | Garis Panduan Pelaksanaan Pengaturcaraan Sistem Aplikasi | Pusat Pembangunan Maklumat dan Komunikasi |
| 19. | -OPR/iDEC/GP07/ IMPLEMENTASI APLIKASI | Garis Panduan Pelaksanaan Implementasi Aplikasi | Pusat Pembangunan Maklumat dan Komunikasi |
| 20. <u>18.</u> | UPM/OPR/BKU/P001 | Prosedur Kawalan Akses | Bahagian Keselamatan Universiti |
| 21. <u>19.</u> | UPM/SOK/PYG/P002 | Prosedur Penyelenggaraan Berkala | Pejabat Pembangunan dan Pengurusan Aset |
| <u>20.</u> | <u>UPM/OPR/iDEC/AK31</u> | <u>Arahan Kerja Perkhidmatan Sokongan ICT</u> | <u>Pusat Pembangunan Maklumat dan Komunikasi</u> |
| <u>21.</u> | <u>OPR/iDEC/GP05/ Pengujian Aplikasi</u> | <u>Garis Panduan Pelaksanaan Pengujian Sistem Aplikasi</u> | <u>Pusat Pembangunan Maklumat dan Komunikasi</u> |
| <u>22.</u> | <u>OPR/PKU/GP13/eKlinik-ID</u> | <u>Garis Panduan Pengurusan Identiti Pengguna ID eKlinik</u> | <u>Pusat Kesihatan Universiti</u> |

Kemaskini: 01 Disember 2021



**LAPORAN SOAL SELIDIK PENDAFTARAN PELAJAR BAHARU
PRASISWAZAH SEMASA MINGGU PERKASA PUTRA BAGI SESI
KEMASUKAN 2021/2022**

KAMPUS SERDANG DAN BINTULU

1.0 TUJUAN

Kertas ini ini bertujuan untuk memaklumkan ahli Mesyuarat Jawatankuasa Kerja ISMS berkaitan Laporan Soal Selidik Pendaftaran Pelajar Baharu Prasiswazah Semasa Minggu Perkasa Putra Pada Sesi Kemasukan 2021/2022.

2.0 LATAR BELAKANG

Tujuan pelaksanaan soal selidik ini adalah untuk mengetahui tahap penerimaan kerahsiaan, integriti, kebolehsediaan dan kepuasan perkhidmatan pendaftaran dalam kalangan pelajar baharu. Persepsi pelajar baharu yang juga merupakan pemegang taruh ini akan mencerminkan tahap pelaksanaan Sistem Pengurusan Keselamatan Maklumat (ISMS) dalam proses pendaftaran pelajar baharu di Universiti Putra Malaysia.

3.0 OBJEKTIF KAJIAN

Objektif kajian ini dilakukan adalah untuk mendapat maklum balas pemegang taruh (Pelajar Baharu) berkenaan pelaksanaan ISMS di UPM seperti berikut, iaitu:

- (i) Mendapatkan maklum balas pelajar baharu berkenaan tahap ketepatan maklumat yang dinyatakan dalam surat tawaran yang dikeluarkan kepada calon;
- (ii) Mendapatkan maklum balas pelajar baharu berkenaan tahap kesediaan kaunter semasa hari pendaftaran pelajar baharu;
- (iii) Mendapatkan maklum balas pelajar baharu berkenaan kawalan kerahsiaan data dan maklumat pelajar baharu semasa hari pendaftaran pelajar; dan
- (iv) Memenuhi keperluan MS ISO/IEC 27001:2013 *Information Security Management System* (ISMS).

4.0 METODOLOGI PELAKSANAAN

Soal selidik kajian ini dijalankan secara atas talian untuk pelajar baharu UPM ambilan pertama dan kedua.

Soal selidik secara atas talian ini merangkumi 2 bahagian seperti berikut, iaitu:

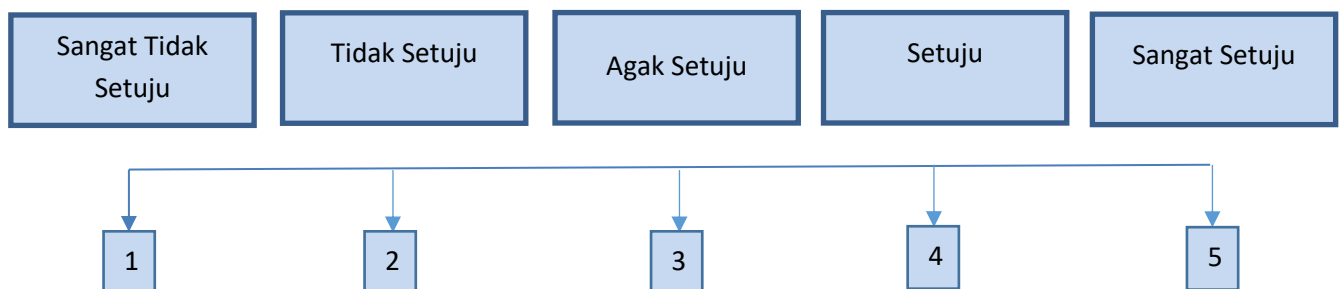
Bahagian A: Maklumat Demografi Responden

- (i) Jantina; dan
- (ii) Kolej Kediaman.

Bahagian B: Soalan Soal Selidik Kepuasan Pemegang Taruh Terhadap Perkhidmatan atau perkara berikut:

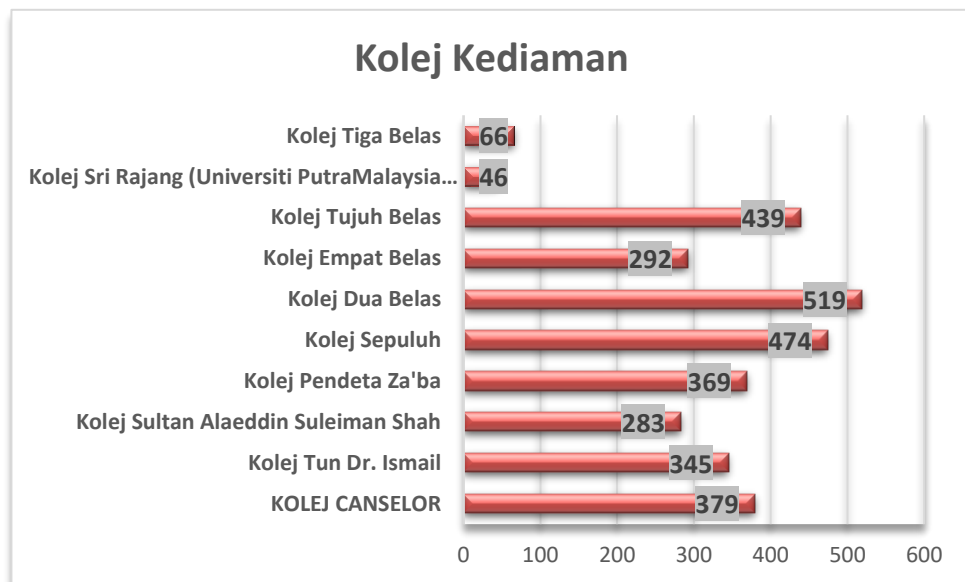
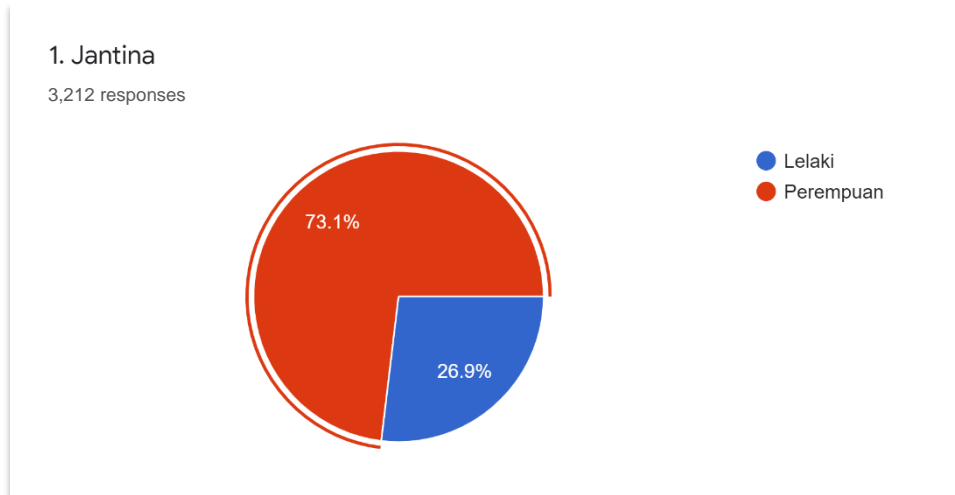
- (i) Saya dapati maklumat dalam surat tawaran universiti khususnya nama, no. kad pengenalan dan alamat surat-menyurat adalah tepat.
- (ii) Saya yakin maklumat peribadi saya akan digunakan untuk tujuan pendaftaran dan urusan berkaitan di Universiti Putra Malaysia sahaja.
- (iii) Saya yakin Universiti Putra Malaysia melindungi semua data peribadi saya dan tidak mendedahkan kepada pihak lain yang tidak berkaitan.
- (iv) Saya yakin kerahsiaan data peribadi yang telah saya muat naik ke dalam Sistem e-Daftar SMP terpelihara.
- (v) Saya dapati Sistem e-Daftar SMP boleh dicapai sepanjang tempoh pendaftaran.
- (vi) Saya mendapati Sistem e-Daftar SMP memudahkan proses pendaftaran masuk ke Universiti Putra Malaysia.
- (vii) Cadangan penambahbaikan/maklum balas berkaitan keselamatan maklumat semasa pendaftaran (jika ada).

Responden diminta memberikan penarafan mata mengikut skala kepuasan terhadap perkhidmatan yang diberikan seperti berikut:



5.0 ANALISIS RESPONDEN

Seramai 3,212 (88.2%) orang pelajar telah menjawab soal selidik yang disediakan berbanding 3,641 pelajar baharu yang mendaftar secara dalam talian (*online*) pada ambilan pertama dan ambilan kedua sesi 2021/2022. Data responden dipecahkan mengikut jantina dan 10 Kolej Kediaman. Analisis responden adalah seperti jadual di bawah:



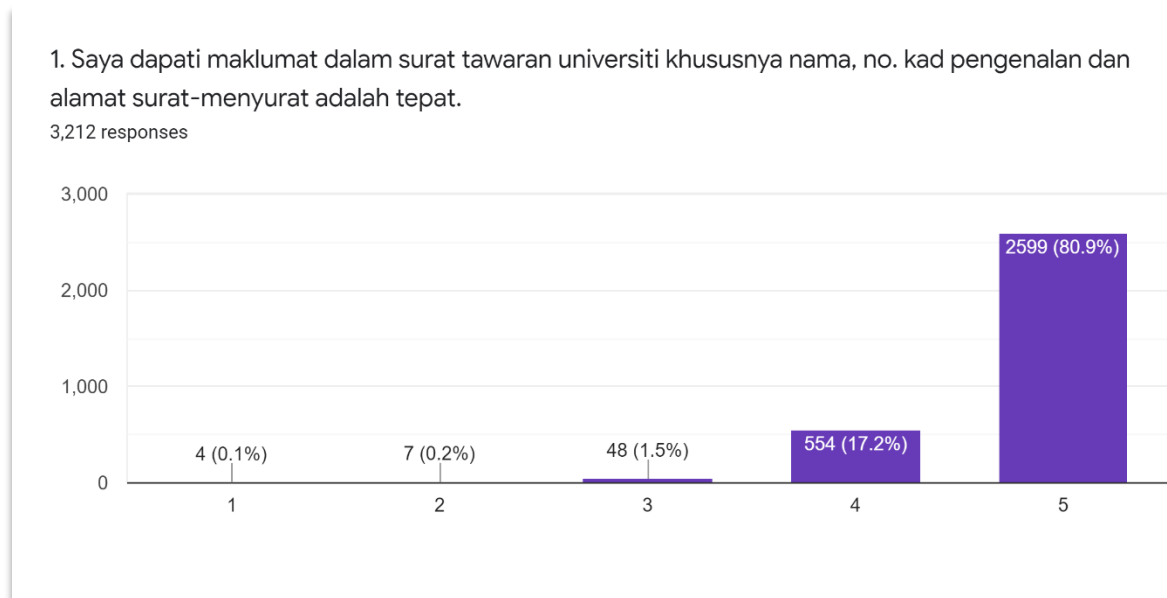
6.0 ANALISIS HASIL KAJIAN

Tahap kepuasan pemegang taruh dianalisis berdasarkan skala kepuasan berikut, iaitu:

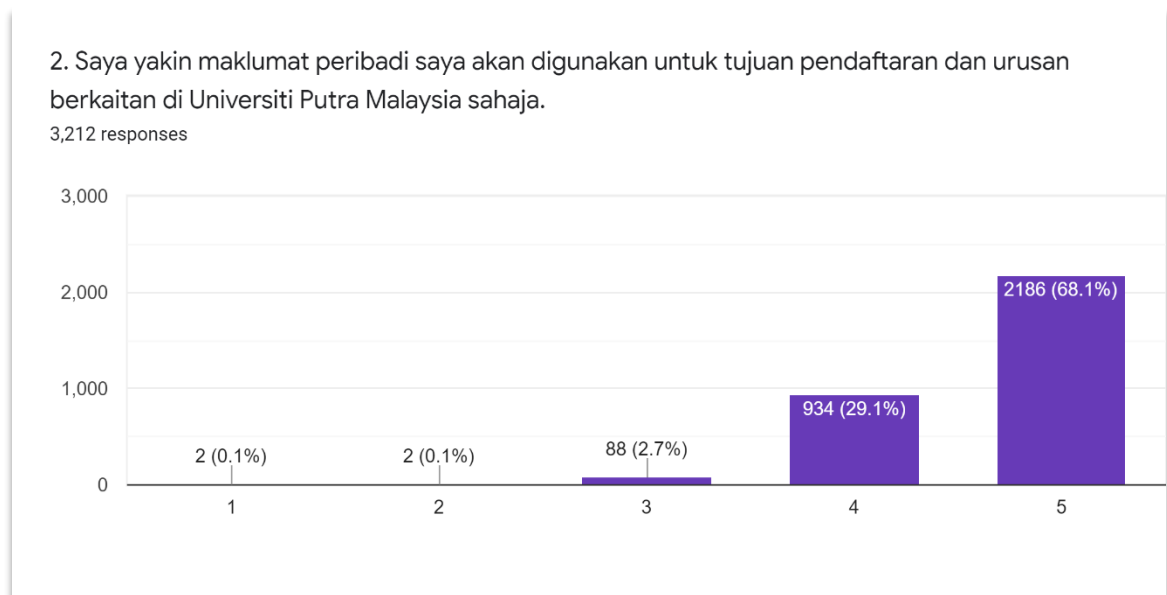
- (i) Skala 5 (Sangat Setuju)
- (ii) Skala 4 (Setuju)
- (iii) Skala 3 (Agak Setuju)
- (v) Skala 2 (Tidak Setuju)
- (vi) Skala 1 (Sangat Tidak Setuju)

Kepuasan pemegang taruh adalah dikira berdasarkan skala kepuasan melebihi tahap memuaskan iaitu merangkumi skala 4 (Setuju) dan skala 5 (Sangat Setuju). Keputusan hasil kajian adalah seperti rajah I hingga IV seperti di bawah:

Rajah I: Soalan i



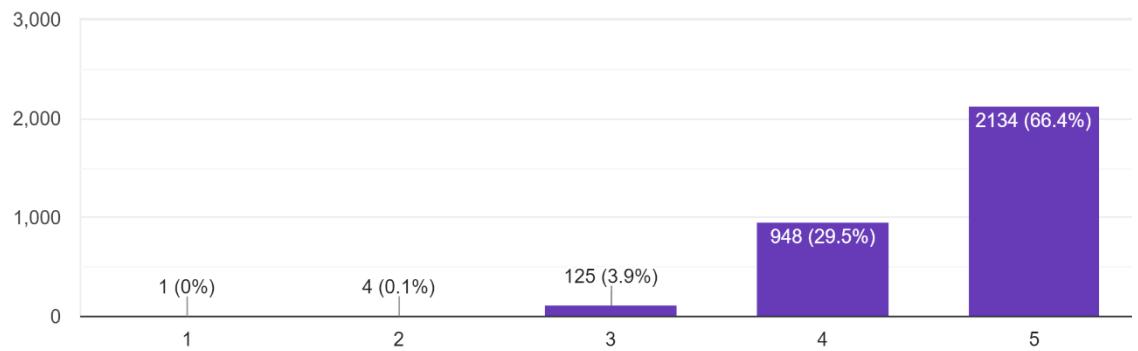
Rajah II: Soalan ii



Rajah III: Soalan iii

3. Saya yakin Universiti Putra Malaysia melindungi semua data peribadi saya dan tidak mendedahkan kepada pihak lain yang tidak berkaitan.

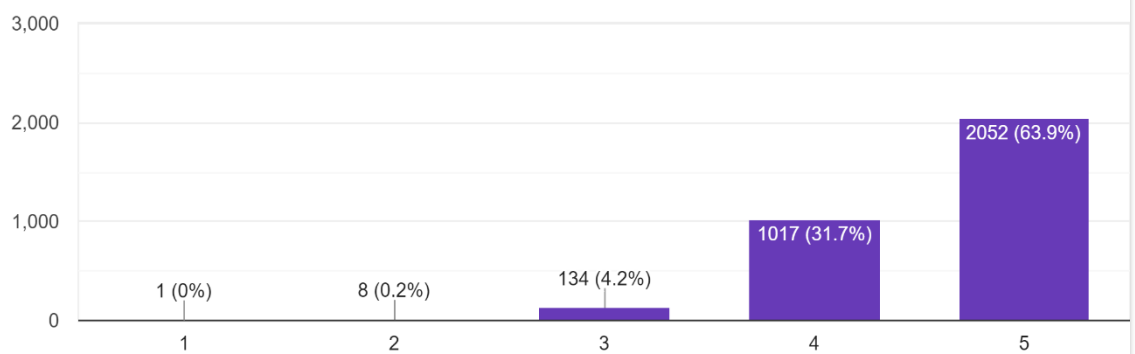
3,212 responses



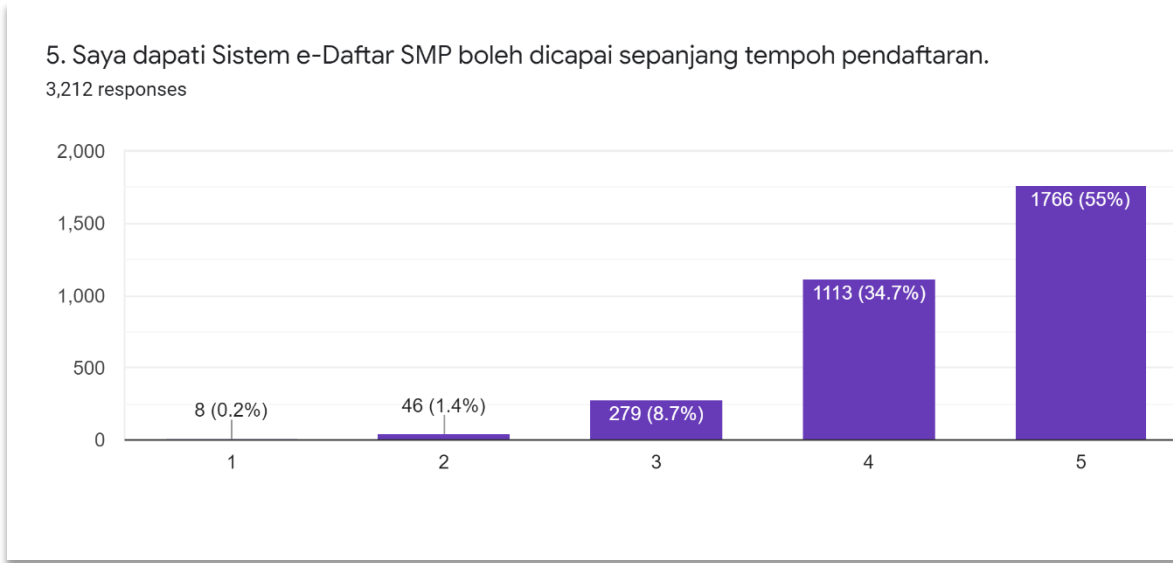
Rajah IV: Soalan iv

4. Saya yakin kerahsiaan data peribadi yang telah saya muat naik ke dalam Sistem e-Daftar SMP terpelihara.

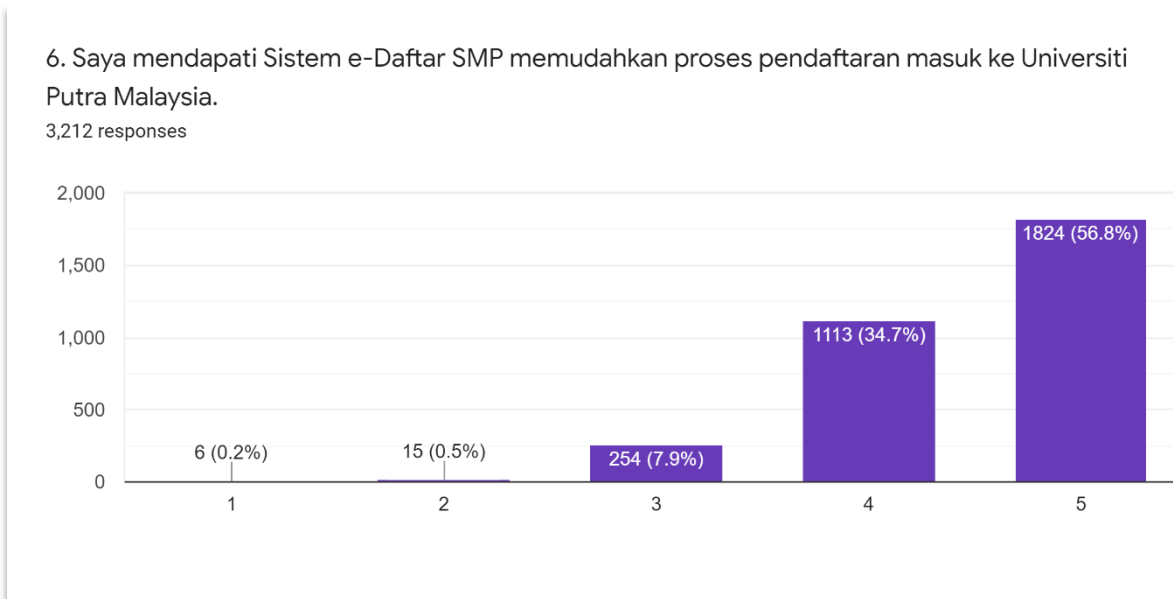
3,212 responses



Rajah V: Soalan v



Rajah VI: Soalan VI



Soalan VIII - Cadangan penambahbaikan / maklum balas berkaitan keselamatan maklumat semasa pendaftaran (jika ada).

Berdasarkan kepada maklumbalas responden bagi soalan kaji selidik ISMS, terdapat beberapa cadangan yang boleh diambil kira oleh Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang untuk tindakan penambahbaikan pada masa akan datang.

Antara cadangan penambahbaikkkan yang diperolehi daripada responden (Pelajar Baharu) :

1. Memastikan pelajar dapat membuat semakan semula tentang maklumat supaya segala maklumat dapat diisi dengan tepat
2. Diharapkan pihak UPM dapat menguatkan tahap keselamatan digital pada server yang berkaitan supaya tidak berlaku sebarang penyelewengan data yang tidak diingini
3. Meningkatkan lagi tahap keselamatan maklumat peribadi dengan menambah bilangan sekuriti di dalam sistem yang dibangunkan.

Antara komen responden yang perlu diberi perhatian adalah seperti berikut:

1. Terdapat kesalahan maklumat pada e-daftar (maklumat alamat rumah dan juga nombor telefon).
2. Memelihara maklumat pelajar dengan menyediakan sistem keselamatan e daftar yang sangat ketat.
3. Mempertingkatkan sistem perlindungan maklumat peribadi daripada digodam oleh penggodam.
4. Pihak UPM perlu menyediakan link group Telegram atau WhatsApp yang mempunyai kawalan rapi agar scammer tidak sesuka hati mencero boh masuk ke dalam mana-mana *group*.
5. Saya pernah mengalami gangguan di WhatsApp disebabkan saya pernah mengisi *google form* berkaitan kolej (semasa Asasi UPM 2020/2021) yang memerlukan saya untuk mengisi nama dan no telefon, beberapa orang yang tidak dikenali pernah menghubungi saya sehingga saya berasa rimas kerana dihubungi oleh orang yang tidak dikenali.
6. Cuba (jika boleh) elakkan bagi kelonggaran kepada pelajar supaya mengisi maklumat melalui *google spreadsheet* yang mana boleh diakses oleh semua pelajar pada satu-satu masa. Hal ini berlaku tadi akibat terdapat kesalahan maklumat pada list Penasihat Akademik. Nama, No kad pengenalan, dan no. telefon pelajar telah terdedah kepada pelajar lain. Saya faham situasi seperti ini tidak dapat dielakkan.

Terdapat juga hasil responden yang memberi penghargaan kepada sistem e-daftar SMP yang baru diperkenalkan :

1. Bagi saya, sistem ini sangat tersusun dan sangat mudah diisi. Saya tidak mempunyai isu berkaitan dengan keselamatan maklumat semasa pendaftaran.

7.0 RUMUSAN HASIL KAJIAN

Secara keseluruhan, hasil soal selidik pendaftaran pelajar baharu prasiswazah semasa Minggu Perkasa Putra pada sesi kemasukan Semester 1 sesi 2021/2022 dapat dirumuskan seperti berikut:

Peratusan pelajar yang menjawab soal selidik ini meningkat sebanyak **24.16%** berbanding tahun 2020. Ia mungkin disebabkan strategi meletakkan pautan soal selidik ISMS di dalam E-Daftar seperti cadangan penambahbaikan yang dinyatakan pada tahun 2020.

Analisis kepuasan pemegang taruh menunjukkan **94.65%** Pelajar Baharu yang mendaftar berpuas hati (skala 4 dan skala 5) dengan semua perkhidmatan yang diberikan semasa hari pendaftaran berdasarkan soalan 1 sehingga 6.

Jumlah responden yang tertinggi yang memberikan skala 5 (sangat memuaskan) adalah pada soalan 1 iaitu **'Saya dapati maklumat dalam surat tawaran universiti khususnya nama, no. kad pengenalan dan alamat surat-menyurat adalah tepat.'** (2599 responden). Manakala yang terendah yang memberikan skala 5 adalah pada soalan 5 iaitu **'Saya dapati Sistem e-Daftar SMP boleh dicapai sepanjang tempoh pendaftaran.'** (1766 responden).

Jumlah responden yang tertinggi yang memberikan skala 1 (sangat tidak memuaskan) adalah kepada soalan 5 iaitu **'Saya dapati Sistem e-Daftar SMP boleh dicapai sepanjang tempoh pendaftaran.'** (8 responden).

8.0 CADANGAN PENAMBAHBAIKAN

Peratusan pelajar berpuashati berkaitan keselamatan dan proses pendaftaran adalah tinggi, namun terdapat juga beberapa komen dan cadangan penambahbaikan yang telah dinyatakan berkaitan isu keselamatan data perlu diberi perhatian untuk penambahbaikan.

9.0 PELAKSANAAN SOAL SELIDIK PIHAK BERKEPENTINGAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT TAHUN 2021

Pelaksanaan soal selidik pihak yang berkepentingan ISMS tahun 2021 dilaksanakan seperti:

- (i) Soal selidik pendaftaran pelajar baharu prasiswazah oleh Peneraju Pendaftaran Pelajar Baharu Prasiswazah (Serdang dan Bintulu), berdasarkan strategi berikut :
 - (a) Soalan kajian yang diajukan adalah berdasarkan tahap kerahsiaan, integriti, kebolehsediaan dan kepuasan perkhidmatan pendaftaran pelajar baharu terhadap jenis perkhidmatan yang diterima daripada setiap peneraju/entiti yang menawarkan perkhidmatan.

- (b) Respon pemegang taruh adalah berdasarkan tahap kepuasan mereka mengikut skala 1 hingga 5 (Skala Likert) yang telah ditetapkan.
- (c) Pelajar baharu prasiswazah sesi 2021/2022 UPM menjawab soal selidik melalui pautan yang diletakkan di dalam sistem E-Daftar.
- (d) Pelaksanaan soal selidik ini akan dilaksanakan oleh Peneraju Proses ISMS yang terlibat iaitu Pejabat Hal Ehwal Pelajar dan Alumni dengan kerjasama Jawatankuasa Penilaian Minggu Perkasa Putra 2021.

10.0 SYOR

Ahli Mesyuarat Jawatankuasa Kerja ISMS dimohon mengambil maklum Laporan Analisis Pelaksanaan Soal Selidik Pendaftaran Pelajar Baharu Prasiswazah Semasa Minggu Perkasa Putra bagi Sesi 2021/2022 seperti yang dikemukakan.