HURAIAN PINDAAN DOKUMEN ISO UPM

BAHAGIAN A: Huraian Pindaan Dokumen ISO
(Diisi oleh Pemohon/Pemilik Proses dan sila abaikan ruangan No. CPD kerana akan dilengkapkan oleh TPKD PP)

No. CPD	Pemilik Proses	Huraian Pindaan Dokumen *		Tambahan (T) / ~~Pemotongan~~ (P)
		Asal	**Pindaan**	
ISMS (SOK): IDEC 1/2019	**iDEC**	Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT Kod Dokumen: UPM/ISMS/SOK/P001 No. Isu:_01_, No. Semakan:_02_, Tarikh Kuatkuasa: 13/10/2017	Nama Dokumen: PROSEDUR PELAN TINDAK BALAS INSIDEN ICT Kod Dokumen: UPM/ISMS/SOK/P001 No. Isu:_01_, No. Semakan:_03_, Tarikh Kuatkuasa: 22/02/2019	
		1.0 TUJUAN Prosedur ini ~~bagi menerangkan gambaran apakah maksud insiden dan pelan tindak balas insiden membincangkan bagaimana maklumat disalurkan kepada personal terlibat, penilaian terhadap insiden, mengurangkan kerosakan dan strategi tindak balas, dokumentasi dan menyimpan bukti.~~	**1.0 TUJUAN** Prosedur ini disediakan bagi tujuan menerangkan kaedah mengendalikan insiden keselamatan ICT atau pelanggaran keselamatan bagi meminimumkan kerosakan akibat insiden keselamatan ICT dan kegagalan fungsi (*malfunction*).	**P/T**
		~~**2.0 OBJEKTIF**~~ ~~Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.~~	**2.0 SKOP** Prosedur ini merangkumi semua proses melapor, merekodkan insiden keselamatan ICT, mengenal pasti bagaimana ianya berlaku serta memulih dan memastikan kelangsungan operasi.	**P/T**
		~~**3.0 SKOP**~~ ~~Prosedur ini merangkumi proses pelaporan insiden, menyelenggara atau memulih kelangsungan operasi, mengenal pasti bagaimana insiden berlaku, memastikan insiden tidak berulang dan pengurusan maklumat insiden.~~	**3.0 TANGGUNGJAWAB** Pengarah iDEC bertanggungjawab memastikan prosedur ini dilaksanakan. Sesiapa yang terlibat perlu mematuhi prosedur ini.	**P/T**

		4.0 DOKUMEN RUJUKAN ~~UPM/ISMS/OPR/ GP18/PENGENDALIAN INSIDEN~~ – ~~Garis Panduan Pengendalian Insiden ICT~~ ~~DRP-ICT UPM (3.0)~~ – ~~Pelan Pemulihan Bencana ICT UPM~~ ~~Bilangan 4 Tahun 2006~~ – ~~Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.~~ ~~Bilangan 1 Tahun 2001~~ – ~~Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi~~	**4.0 DOKUMEN RUJUKAN** Bilangan 4 Tahun 2006 – Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam. Bilangan 1 Tahun 2001 – Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi - – Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK) DRP-ICT UPM (3.0) – Pelan Pemulihan Bencana ICT UPM UPM/ISMS/OPR/ GP18/PENGENDALIAN INSIDEN – Garis Panduan Pengendalian Insiden ICT	**P/T**

Kod Dokumen	Tajuk Dokumen
~~UPM/ISMS/OPR/ GP18/PENGENDALIAN INSIDEN~~	~~Garis Panduan Pengendalian Insiden ICT~~
~~DRP-ICT UPM (3.0)~~	~~Pelan Pemulihan Bencana ICT UPM~~
~~Bilangan 4 Tahun 2006~~	~~Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.~~
~~Bilangan 1 Tahun 2001~~	~~Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi~~

Kod Dokumen	Tajuk Dokumen
Bilangan 4 Tahun 2006	Surat Pekeliling Am Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.
Bilangan 1 Tahun 2001	Pekeliling Am Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi
-	Garis Panduan Keselamatan Teknologi Maklumat & Komunikasi (GPKTMK)
DRP-ICT UPM (3.0)	Pelan Pemulihan Bencana ICT UPM
UPM/ISMS/OPR/ GP18/PENGENDALIAN INSIDEN	Garis Panduan Pengendalian Insiden ICT

		~~**5.0 MEKANISMA PELAPORAN**~~ ~~Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Insiden adalah salah satu atau lebih perkara yang tersenarai dibawah berlaku:~~ ~~i. Kehilangan data.~~ ~~ii. Kerosakan data.~~ ~~iii. Kehilangan aset ICT.~~ ~~iv. Kerosakan aset ICT.~~ ~~v. Perkidmatan yang disekat.~~ ~~vi. Salah guna perkhidmatan, maklumat atau aset.~~ ~~vii. Sistem dijangkiti virus atau sebarang ancaman.~~ ~~viii. Percubaan untuk membuat capaian yang tidak dibenarkan.~~ ~~ix. Perubahan yang tidak dibenarkan.~~ ~~Sebarang insiden keselamatan ICT hendaklah dilaporkan kepada Pemilik Proses dengan kadar segera jika:~~ ~~i. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;~~ ~~ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;~~ ~~iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;~~ ~~iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan maklumat/data, sistem kerap kali gagal dan komunikasi tersalah hantar; dan~~ ~~v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.~~	**5.0 TERMINOLOGI DAN SINGKATAN** ICT : Teknologi Maklumat dan Komunikasi iDEC : Pusat Pembangunan Maklumat Dan Komunikasi JKKTMK : Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Pekerja ICT : Pegawai Teknologi Maklumat / Jurutera / Penolong Pegawai Teknologi Maklumat / Penolong Jurutera / Juruteknik Komputer / Pekerja lain yang dilantik untuk mengurus ICT Pengarah iDEC : Pengarah Pusat Pembangunan Maklumat Dan Komunikasi Pentadbir Sistem : Pekerja Teknikal ICT yang memelihara keselamatan, menyelenggara, atau mengawal sesuatu aset Penyelia : Pekerja yang menyelia Pekerja ICT PYB : Pegawai yang bertanggungjawab TPKD : Timbalan Pegawai Kawalan Dokumen TWP : Timbalan Wakil Pengurusan UPMCERT : UPM *Computer Emergency Response Team* WP : Wakil Pengurusan	**P/T**

~~**6.0 PENGURUSAN INSIDEN KESELAMATAN ICT**~~

~~**6.1 PENGENDALIAN MAKLUMAT INSIDEN KESELAMATAN ICT**~~

~~Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Universiti Putra Malaysia.~~

~~Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Rujuk Garis Panduan Pengendalian Insiden ICT (UPM/ISMS/OPR/GP18/PENGENDALIAN INSIDEN).~~

~~**6.2 PELAN TINDAK BALAS INSIDEN KESELAMATAN ICT**~~

~~**Proses**~~	~~**Aktiviti**~~	~~**Masa**~~	~~**Tindakan**~~
~~Pemeriksaan~~	~~a. Mengenal pasti status/situasi bagi:~~ ~~- Perkakas yang terlibat telah mengalami kerosakan dan tidak boleh dibaik pulih~~ ~~- Wujud gangguan capaian pada rangkaian/emel/system berbanding keadaan normal.~~ ~~b. Membuat troubleshoot / pengujian terhadap isu berkenaan.~~ ~~c. Mendapatkan khidmat nasihat pihak ketiga (jika perlu) untuk membuat keputusan bagi kaedah pemulihan terbaik~~	~~Serta merta~~	~~Pentadbir Sistem~~

6.0 PROSES TERPERINCI

Tanggung jawab	Carta Alir		Perincian	Rekod/ Dokumen Rujukan
	6.1 Mula			
PYB	6.2 Terima aduan insiden ICT	6.2	Menerima aduan daripada saluran yang betul atau daripada Pentadbir Sistem	
Pekerja ICT	6.3 Laksanakan siasatan terhadap kes insiden ICT yang diterima	6.3	Pekerja ICT menggunakan perisian sokongan untuk menganalisa log yang berkaitan terhadap kes insiden ICT yang diterima dengan langkah seperti berikut: (a) Menganalisis dan mengenal pasti punca kejadian; dan (b) Mengumpul jejak audit dan bukti berkaitan.	
Penyelia / Pentadbir Sistem / Pekerja ICT	6.4 Laporkan penemuan siasatan kepada UPMCERT, JKKTMK dan Pentadbir Sistem	6.4	6.4.1 Laporan penemuan insiden ICT hasil siasatan mengandungi perancangan dan pelaksanaan baik pulih untuk mengelak kejadian daripada berulang.	
			6.4.2 Laporan Insiden ICT:	
			(a) Pentadbir Sistem perlu membuat permohonan perkhidmatan ICT melalui sistem Perkhidmatan ICT (SPICT)	SPICT
			(b) Pekerja ICT perlu mengisi laporan pada Borang Maklumat Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.0)	Borang Maklumat Pengendalian Insiden Keselamatan ICT
			(c) Pentadbir Sistem perlu mengisi Borang Maklumbalas Tindakan Susulan dari Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.1)	Borang Maklumbalas Tindakan Susulan dari Pengendalian Insiden Keselamatan ICT
			6.4.3 Laporan Imbasan :	
			(a) Pekerja ICT perlu mengisi Borang Maklumat Imbasan *Server/Host* (UPM/ISMS/OPR/IRH 2.0)	Borang Maklumat Imbasan *Server/ Host*
			(b) Pentadbir Sistem perlu mengisi Borang Maklumbalas Tindakan Susulan Imbasan *Server/ Host* (UPM/ISMS/OPR/IRH 2.1)	Borang Maklumbalas Tindakan Susulan Imbasan *Server/Host*
Pekerja ICT	6.5 Rekod insiden ICT yang diterima ke dalam fail	6.5	6.5.1 Semua insiden ICT yang berlaku hendaklah direkodkan ke dalam fail dan mempunyai nombor log sebagai rujukan	
			6.5.2 Semua insiden keselamatan ICT yang dikesan hendaklah mempunyai sekurang-kurangnya maklumat seperti berikut: (a) Tarikh dan masa insiden ICT; (b) Menyenaraikan sistem yang terjejas akibat insiden atau kejadian tersebut; (c) Ringkasan insiden ICT; (d) Tindakan yang diambil untuk membetulkan insiden ICT; (e) Senarai bukti yang diperolehi semasa siasatan; dan (f) Pengajaran yang diperolehi	
	6.6 Tamat			

P/T

		~~Membuat hebahan~~	~~a. Memaklumkan kepada pengguna mengenai insiden yang berlaku menerusi kaedah seperti:~~ ~~- Emel/ laman web / sistem~~ ~~- Surat/memo rasmi/Lisan~~ ~~b. Melaporkan kepada Jawatankusa Komunikasi Krisis bagi aktiviti komunikasi dengan media.~~	~~Serta merta~~	~~Pentadbir Sistem~~ ~~Pengarah iDEC~~			
		~~Pembaikan~~	~~a. Pembaikan dalaman menggunakan kepakaran pegawai teknologi maklumat dan sumber sedia ada.~~ ~~b. Pembaikan luaran dengan mendapatkan kepakaran luaran dan memastikan keselamatan data terjamin.~~ ~~c. Tindakan pemulihan ke atas bencana berkaitan ICT hendaklah merujuk kepada manual:~~ ~~- Pelan Pemulihan Bencana ICT UPM~~	~~Serta merta~~ ~~Mengikut masa yang ditetapkan~~	~~Pentadbir Sistem~~ ~~Pentadbir Sistem~~ ~~Pengarah iDEC~~			
		~~Pemantauan~~	~~a. Pemeriksaan berkala bagi memastikan perkhidmatan ICT berjalan seperti biasa. Rujuk Prosedur Penyelenggaraan ICT *(UPM/OPR/IDEC/P003)*~~	~~Berjadual~~	~~Pentadbir Sistem~~ ~~Pentadbir~~			

			. b. Memberi kesedaran kepada pengguna terhadap langkah menjamin keselamatan dan proses kerja bagi perkhidmatan ICT. Rujuk Garis Panduan Keselamatan Teknologi Maklumat Komunikasi. c. Mendapatkan maklum balas dari pengguna berkenaan perkhidmatan ICT(cadangan penambahbaikan, aduan dll). d. Menyediakan laporan insiden dan makluman kepada Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi UPM		Sistem Pentadbir Sistem Pengarah iDEC			

7.0 REKOD ~~KUALITI~~

Bil	Kod Fail, Tajuk Fail dan Senarai Rekod	Tanggungjawab Mengumpul dan Memfail	Tanggungjawab Menyelenggara	Tempat dan Tempoh Simpanan
1.	UPM/100-4/12/19 Pengendalian Insiden • Permohonan Perkhidmatan ICT (melalui Sistem Perkhidmatan ICT (SPICT)) • Borang Maklumat Pengendalian Insiden Keselamatan ICT ~~(Borang IRH 1.0)~~ • Borang Maklumbalas Tindakan Susulan dari Pengendalian Insiden Keselamatan ICT ~~(Borang IRH 1.1)~~ • Borang ~~Maklumat~~ Imbasan server/Host ~~(Borang IRH 2.0)~~ • Borang Maklumbalas Tindakan Susulan dari Imbasan Server/Host ~~(Borang IRH (2.1)~~	~~Staf SRK~~	~~Ketua SRK~~	SRK 3 Tahun

7.0 REKOD

Bil	Kod Fail, Tajuk Fail dan Senarai Rekod	Tanggungjawab Mengumpul dan Memfail	Tanggungjawab Menyelenggara	Tempat dan Tempoh Simpanan
1.	UPM/100-4/12/19 **Pengendalian Insiden ICT** • Permohonan Perkhidmatan ICT (melalui Sistem Perkhidmatan ICT (SPICT)) • Borang Maklumat Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.0) • Borang Maklumbalas Tindakan Susulan dari Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.1) • Borang Imbasan *Server/Host* (UPM/ISMS/OPR/IRH 2.0) • Borang Maklumbalas Tindakan Susulan dari Imbasan *Server/Host* (UPM/ISMS/OPR/IRH 2.1)	Pekerja ICT	Penyelia	Rak Fail 3 Tahun

P/T

8.0 SEJARAH SEMAKAN

No. Isu	No. Semakan	No. CPD	Kelulusan Mesyuarat	Disedia dan Disemak	Dilulus/ diluluskan semula	Tarikh Kuatkuasa
01	00	25/2012	Keluaran Pertama	Pengarah iDEC	WP	30/11/2012
01	01	ISMS (SOK) : iDEC 02/2016	Mesyuarat Jawatankuasa Kerja ISMS kali ke-2	TPKD	TWP ISMS	01/07/2016
01	02	ISMS (SOK) : iDEC 05/2016	Mesyuarat Jawatankuasa Pengurusan ISO iDEC Kali Ke-2	TPKD	TWP PP	13/10/2017

8.0 SEJARAH SEMAKAN

No. Isu	No. Semakan	No. CPD	Kelulusan Mesyuarat	Disedia dan Disemak	Dilulus/ diluluskan semula	Tarikh Kuatkuasa
01	00	25/2012	Keluaran Pertama	Pengarah iDEC	WP	30/11/2012
01	01	ISMS (SOK) : iDEC 02/2016	Mesyuarat Jawatankuasa Kerja ISMS kali ke-2	TPKD	TWP ISMS	01/07/2016
01	02	ISMS (SOK) : iDEC 05/2016	Mesyuarat Jawatankuasa Pengurusan ISO iDEC Kali Ke-2	TPKD	TWP PP	13/10/2017
01	03	ISMS (SOK): IDEC-1/2019	Mesyuarat Jawatankuasa Pengurusan iDEC ke- 104 (Bil. 2/2019)	TPKD PP	TWP PP	22/02/2019

T

BAHAGIAN B: Kelulusan CADANGAN PINDAAN DOKUMEN ISO
(Diisi oleh PKD / TPKD mengikut skop dokumen ISO)

Peneraju Proses:	**PUSAT PEMBANGUNAN MAKLUMAT & KOMUNIKASI (iDEC)**		
Kelulusan Mesyuarat:	**MESYUARAT JAWATANKUASA PENGURUSAN iDEC**	**Kali ke-**	**104 (Bil 2/2019)**
Tarikh Mesyuarat:	**1 FEBRUARI 2019**		
Cadangan Tarikh Kuatkuasa *:	**22 FEBRUARI 2019**		

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