



POLISI KESELAMATAN SIBER  
MIROS

MIROS/ITM/SPL/ICT/POL01

Tarikh Kuat Kuasa:

01 April 2024

Versi: 2.0

Muka Surat: 1/78

---

# POLISI KESELAMATAN SIBER (PKS) MIROS

---

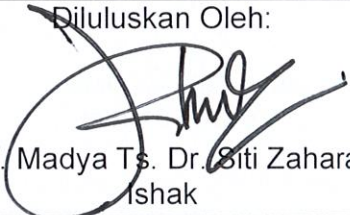
Disediakan Oleh:

  
Ts. Nor Azlan Bin Ahmad  
Ketua Unit Pengurusan Teknologi  
Maklumat

Disemak Oleh:

  
Ts. Mohd Zakry Bin Omar  
Ketua Bahagian Khidmat Pengurusan

Diluluskan Oleh:

  
Prof. Madya Ts. Dr. Siti Zaharah  
Ishak

Unit Pengurusan Teknologi Maklumat  
Bahagian Khidmat Pengurusan  
MIROS

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p align="center"><b>POLISI KESELAMATAN SIBER</b></p> <p align="center"><b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 2/78

## KANDUNGAN

<b>1.0 PENGENALAN</b>	<b>7</b>
<b>2.0 OBJEKTIF</b>	<b>7</b>
<b>3.0 PERLANTIKAN</b>	<b>7</b>
<b>4.0 PERNYATAAN DASAR</b>	<b>8</b>
<b>5.0 SKOP</b>	<b>9</b>
<b>6.0 PRINSIP-PRINSIP</b>	<b>11</b>
<b>BIDANG 01 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR</b>	<b>14</b>
<b>0101 Dasar Keselamatan ICT</b>	<b>14</b>
010101 Pelaksanaan Dasar	14
010102 Penyebaran Dasar	14
010103 Penyelenggaraan Dasar	14
010104 Pengecualian Dasar	15
<b>BIDANG 02 - ORGANISASI KESELAMATAN</b>	<b>15</b>
<b>0201 Infrastruktur Organisasi Dalaman</b>	<b>15</b>
020101 Ketua Jabatan	15
020102 Ketua Pegawai Digital (CDO)	15
020103 Pegawai Keselamatan ICT (ICTSO)	16
020104 Pengurusan ICT	17
020105 Pentadbir Sistem ICT	17
020106 Pengguna	18
020107 Jawatankuasa Keselamatan ICT (JKICT) MIROS	19
020108 Pasukan Tindak Balas Insiden Keselamatan Siber MOT (CSIRTMOT)	20
<b>0202 Pihak Ketiga</b>	<b>21</b>
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	21
<b>BIDANG 03 - PENGURUSAN ASET ICT</b>	<b>22</b>
<b>0301 Akauntabiliti Aset</b>	<b>22</b>
030101 Inventori Aset ICT	22
<b>0302 Pengelasan dan Pengendalian Maklumat</b>	<b>23</b>

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 3/78

030201 Pengelasan Maklumat .....	23
030202 Pengendalian Maklumat .....	24
<b>BIDANG 04 - PENGURUSAN OPERASI DAN KOMUNIKASI</b>	<b>24</b>
<b>0401 Pengurusan Prosedur Operasi.....</b>	<b>24</b>
040101 Pengendalian Prosedur .....	25
040102 Kawalan Perubahan .....	25
040103 Pengasingan Tugas dan Tanggungjawab .....	26
<b>0402 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga .....</b>	<b>26</b>
040201 Perkhidmatan Penyampaian .....	27
<b>0403 Perancangan dan Penerimaan Sistem.....</b>	<b>27</b>
040301 Perancangan Kapasiti.....	27
040302 Penerimaan Sistem .....	27
<b>0404 Perisian Berbahaya .....</b>	<b>28</b>
040401 Perlindungan dari Perisian Berbahaya .....	28
040402 Perlindungan dari <i>Mobile Code</i> .....	29
<b>0405 Housekeeping.....</b>	<b>29</b>
040501 <i>Backup</i> .....	29
<b>0406 Pengurusan Rangkaian .....</b>	<b>30</b>
040601 Kawalan Infrastruktur Rangkaian .....	30
<b>0407 Pengurusan Media .....</b>	<b>31</b>
040701 Penghantaran dan Pemindahan .....	31
040702 Prosedur Pengendalian Media.....	31
<b>0408 Pengurusan Pertukaran Maklumat.....</b>	<b>32</b>
040801 Pertukaran Maklumat.....	32
040802 Pengurusan Mel Elektronik (E-mel).....	32
<b>0409 Perkhidmatan E-Dagang (<i>Electronic Commerce Services</i>) .....</b>	<b>33</b>
040901 E-Dagang .....	33
040902 Maklumat Umum.....	33
<b>0410 Pemantauan.....</b>	<b>34</b>
041001 Pengauditan dan Forensik ICT .....	34
041002 Jejak Audit.....	35

041003 Sistem Log.....36  
041004 Pemantauan Log .....36

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 4/78

<b>BIDANG 05 - KAWALAN CAPAIAN</b>	<b>37</b>
<b>0501 Dasar Kawalan Capaian</b> .....	<b>37</b>
050101 Keperluan Kawalan Capaian.....	37
<b>0502 Pengurusan Capaian Pengguna</b> .....	<b>37</b>
050201 Akaun Pengguna .....	38
050202 Hak Capaian.....	39
050203 Pengurusan Kata Laluan .....	39
050204 Clear Desk dan Clear Screen .....	40
<b>0503 Kawalan Capaian Rangkaian</b> .....	<b>40</b>
050301 Capaian Rangkaian .....	40
050302 Capaian Internet .....	41
050303 Capaian Jarak Jauh.....	42
<b>0504 Kawalan Capaian Sistem Pengoperasian</b> .....	<b>43</b>
050401 Capaian Sistem Pengoperasian.....	43
<b>0505 Kawalan Capaian Aplikasi dan Maklumat</b> .....	<b>44</b>
050501 Capaian Aplikasi dan Maklumat.....	44
<b>0506 Peralatan Mudah Alih dan Kerja Jarak Jauh</b> .....	<b>45</b>
050601 Peralatan Mudah Alih.....	45
050602 Kerja Jarak Jauh.....	45
<b>BIDANG 06 : KESELAMATAN SUMBER MANUSIA</b>	<b>45</b>
<b>0601 Keselamatan Sumber Manusia Dalam Tugas Harian</b> .....	<b>45</b>
060101 Sebelum Perkhidmatan.....	46
060102 Dalam Perkhidmatan .....	46
060103 Bertukar Atau Tamat Perkhidmatan .....	47
<b>BIDANG 07 - KESELAMATAN FIZIKAL DAN PERSEKITARAN</b>	<b>47</b>
<b>0701 Keselamatan Kawasan</b> .....	<b>47</b>
070101 Kawalan Kawasan .....	47
070102 Kawalan Masuk Fizikal .....	49
070103 Kawasan Larangan.....	49
<b>0702 Keselamatan Peralatan</b> .....	<b>49</b>

070201 Peralatan ICT .....50  
070202 Media Storan ..... 51

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 5/78

070203 Media Tandatangan Digital .....	53
070204 Media Perisian dan Aplikasi .....	53
070205 Penyelenggaraan Perkakasan .....	54
070206 Peralatan di Luar Premis .....	54
070207 Pelupusan Perkakasan .....	55
<b>0703 Keselamatan Persekitaran .....</b>	<b>56</b>
070301 Kawalan Persekitaran .....	56
070303 Kabel Rangkaian .....	58
<b>0704 Keselamatan Dokumen .....</b>	<b>58</b>
<b>BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM</b>	<b>59</b>
<b>0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi .....</b>	<b>59</b>
080102 Pengesahan Data Input .....	60
080103 Pengesahan Data Output .....	60
<b>0802 Kawalan Kriptografi .....</b>	<b>60</b>
080201 Penyulitan .....	60
080202 Tandatangan Digital .....	60
080303 Pengurusan Infrastruktur Kunci Awam (PKI) .....	60
<b>0803 Keselamatan Fail Sistem .....</b>	<b>60</b>
080301 Kawalan Fail Sistem .....	60
<b>0804 Keselamatan Dalam Proses Pembangunan dan Sokongan .....</b>	<b>61</b>
080402 Pembangunan Secara <i>Outsource</i> .....	62
<b>0805 Kawalan Teknikal Keterdedahan (Vulnerability) .....</b>	<b>62</b>
080501 Kawalan dari Ancaman Teknikal .....	62
<b>BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN</b>	<b>62</b>
<b>0901 Mekanisme Pelaporan Insiden Keselamatan ICT .....</b>	<b>62</b>
<b>0902 Pengurusan Maklumat Insiden Keselamatan ICT .....</b>	<b>64</b>
<b>BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN</b>	<b>65</b>
<b>1001 Dasar Kesyinambungan Perkhidmatan .....</b>	<b>65</b>
100101 Pelan Kesyinambungan Perkhidmatan .....	65
<b>BIDANG 11 – PEMATUHAN</b>	<b>67</b>
<b>1101 Pematuhan dan Keperluan Perundangan .....</b>	<b>67</b>
<b>1102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal .....</b>	<b>68</b>

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 6/78

<b>1103 Pematuhan Keperluan Audit .....</b>	<b>68</b>
<b>1104 Keperluan Perundangan .....</b>	<b>68</b>
<b>1105 Pelanggaran Dasar .....</b>	<b>68</b>
<b>LAMPIRAN 1</b>	<b>72</b>
<b>LAMPIRAN 2</b>	<b>73</b>
<b>ALIR KERJA PELAPORAN INSIDEN KESELAMATAN ICT MIROS .....</b>	<b>73</b>
<b>LAMPIRAN 3</b>	<b>77</b>
<b>SENARAI PERUNDANGAN DAN PERATURAN.....</b>	<b>77</b>



	<p align="center"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 7/78</p>

## 1.0 PENGENALAN

Polisi Keselamatan Siber Institut Penyelidikan Keselamatan Jalan Raya Malaysia mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini diguna pakai oleh MIROS. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT.

## 2.0 OBJEKTIF

Polisi Keselamatan Siber MIROS diwujudkan untuk menjamin kesinambungan urusan MIROS dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Polisi Keselamatan Siber MIROS ialah seperti berikut:

- (a) Memastikan kelancaran operasi MIROS dan meminimumkan kerosakan atau kemusnahan;
- (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi; dan
- (c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

## 3.0 PERLANTIKAN

Berdasarkan keputusan yang dipersetujui melalui Mesyuarat Eksekutif Bil 6/2014 yang mana mesyuarat bersetuju dengan perlantikan seperti berikut:

- |                                 |                                            |
|---------------------------------|--------------------------------------------|
| 1. Pegawai Pengelas             | : Ketua Pengarah MIROS                     |
| 2. Pegawai Pengelas II          | : Ketua Bahagian Khidmat Pengurusan (KBKP) |
| 3. Pegawai Keselamatan Jabatan  | : Pengerusi JKJK                           |
| 4. Penolong Pegawai Keselamatan | : Timbalan Pengerusi JKJK                  |
| 5. Chief Information Officer    | : Ketua Bahagian Khidmat Pengurusan        |
| 6. ICT Security Officer (ICTSO) | : Ketua Unit Pengurusan Teknologi Maklumat |

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 8/78</p>

#### 4.0 PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- (a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- (b) Memastikan setiap maklumat adalah tepat dan sempurna;
- (c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- (d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Polisi Keselamatan Siber MIROS merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

**(a) Kerahsiaan**

Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

**(b) Integriti**

Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

**(c) Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 9/78

**(d) Kesahihan**

Data dan maklumat hendaklah dijamin kesahihannya; dan

**(e) Ketersediaan**

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.


Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

## 5.0 SKOP

Aset ICT MIROS terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. Polisi Keselamatan Siber MIROS menetapkan keperluan-keperluan asas berikut:

- (a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
- (b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, Polisi Keselamatan Siber MIROS ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara- perkara berikut:

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 10/78</p>

(a) **Perkakasan**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MIROS. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) **Perisian**

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada MIROS;

(c) **Perkhidmatan**

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya.

Contoh :

- i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
- ii. Sistem halangan akses seperti sistem kad akses.
- iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) **Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MIROS. Contoh: Sistem dokumentasi, prosedur operasi, rekod-rekod, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain

(e) **Manusia**

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian agensi bagi mencapai misi dan objektif MIROS. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 11/78</p>

**(f) Premis Komputer Dan Komunikasi**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (e) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

## 6.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber MIROS dan perlu dipatuhi adalah seperti berikut:

**(a) Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

**(b) Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/ atau melihat sahaja. Kelulusan JPICT adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

**(c) Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 12/78</p>

bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
- iii. Menentukan maklumat sedia untuk digunakan;
- iv. Menjaga kerahsiaan kata laluan;
- v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

**(d) Pengasingan**

Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangunan, operasi dan rangkaian;

**(e) Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 13/78</p>

(f) **Pematuhan**

Polisi Keselamatan Siber MIROS hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

(g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

(h) **Saling Bergantungan**

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 14/78

<b>BIDANG 01 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0101 Polisi Keselamatan Siber MIROS</b>	
<b>Objektif:</b> PKS MIROS diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran pelaksanaan operasi MIROS secara berterusan dan meminimumkan kerosakan atau kemusnahan aset ICT.	
<b>010101 Pelaksanaan Polisi</b>	
Ketua Jabatan bertanggungjawab dalam memastikan pelaksanaan PKS dengan cekap dan berkesan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) MIROS atau jawatankuasa yang setara dengannya.	Ketua Jabatan
<b>010102 Penyebaran Polisi</b>	
Dasar ini perlu disebar kepada semua pengguna MIROS (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	ICTSO
<b>010103 Penyelenggaraan Polisi</b>	



<p>Polisi Keselamatan Siber MIROS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi Kerajaan dan kepentingan sosial.</p> <p>Berikut adalah prosedur penyelenggaraan Polisi Keselamatan Siber MIROS:</p> <ul style="list-style-type: none"><li>(a) Kenal pasti dan tentukan perubahan yang diperlukan;</li><li>(b) Kemukakan cadangan pindaan secara bertulis kepada CDO MIROS untuk dibentangkan dalam Mesyuarat JPICT MIROS;</li><li>(c) Perubahan yang telah dipersetujui oleh JPICT MIROS dimaklumkan kepada semua pengguna MIROS; dan</li><li>(d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali</li></ul>	ICTSO
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 15/78

<b>010104 Pengecualian Polisi</b>	
Polisi Keselamatan Siber MIROS adalah terpakai kepada semua pengguna MIROS dan tiada pengecualian diberikan.	Semua


<b>BIDANG 02 - ORGANISASI KESELAMATAN</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0201 Infrastruktur Organisasi Dalam</b>	
<b>Objektif:</b> Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber MIROS.	
<b>020101 Ketua Jabatan</b>	
Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut:  (a) Memastikan semua pengguna mematuhi peruntukan-peruntukan di bawah Polisi Keselamatan Siber MIROS; (b) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan (c) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi Keselamatan Siber MIROS.	Ketua Jabatan
<b>020102 Ketua Pegawai Digital (CDO)</b>	
Jawatan Ketua Pegawai Digital (CDO) bagi MIROS disandang oleh Pengarah/ Ketua Bahagian yang mengetuai Pengurusan Teknologi Maklumat.  Peranan dan tanggungjawab CDO adalah seperti berikut:	CDO


	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 16/78


<ul style="list-style-type: none"> <li>(a) Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;</li> <li>(b) Menentukan keperluan keselamatan ICT;</li> <li>(c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Polisi Keselamatan Siber MIROS serta pengurusan risiko dan pengauditan; dan</li> <li>(d) Bertanggungjawab ke atas perkara-perkara yang berkaitan</li> </ul>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

### 020103 Pegawai Keselamatan ICT (ICTSO)


<p>Jawatan ICTSO bagi MIROS disandang oleh Ketua UPTM atau Pegawai yang bertanggungjawab ke atas ICT.</p> <p>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Merancang, mengurus dan melaksanakan program keselamatan ICT MIROS;</li> <li>(b) Menguatkuasakan pelaksanaan Polisi Keselamatan Siber MIROS;</li> <li>(c) Memberi pendedahan berkenaan Polisi Keselamatan Siber MIROS kepada semua pengguna;</li> <li>(d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber MIROS;</li> <li>(e) Menjalankan pengurusan risiko;</li> <li>(f) Mengambil tindakan pembetulan ke atas hasil penemuan audit;</li> <li>(g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;</li> </ul>	ICTSO
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------


	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
	MIROS/ITM/SPL/ICT/POL01	<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 17/78
Tindak balas Insiden Keselamatan ICT (CERT) MOT sehingga Pasukan Tindak balas Insiden Keselamatan ICT (CERT) MIROS ditubuhkan;		
(i) Mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih dengan segera; dan		
(j) Melaporkan kes-kes pelanggaran Polisi Keselamatan Siber MIROS kepada CDO.		
<b>020104 Pengurusan ICT</b>		
Pengurusan ICT bagi MIROS adalah di bawah tanggungjawab Ketua Unit Pengurusan Teknologi Maklumat (UPTM).		Ketua Unit Pengurusan Teknologi Maklumat (KU PTM)
Peranan dan tanggungjawab di bawah Pengurusan ICT adalah seperti berikut:		
(a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan semasa;		
(b) Menentukan kawalan akses pengguna terhadap aset ICT MIROS;		
(c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CDO MIROS;		
(d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MIROS.		
<b>020105 Pentadbir Sistem ICT</b>		
Pentadbir Sistem ICT di MIROS disandang oleh pegawai yang bertanggungjawab ke atas operasi ICT.		
Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:		Pentadbir Sistem ICT
(a) Mengambil tindakan segera apabila kakitangan berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan		

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 18/78</p>
<p>dalam bidang tugas;</p> <p>(b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam PKS;</p> <p>(c) Memantau aktiviti capaian harian pengguna;</p> <p>(d) Memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;</p> <p>(e) Mengenal pasti aktiviti-aktiviti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan segera;</p> <p>(f) Menyimpan dan menganalisis rekod jejak audit;</p> <p>(g) Menyediakan laporan mengenai aktiviti capaian secara berkala.</p>		
<p><b>020106 Pengguna</b></p>		
<p>Peranan dan tanggungjawab pengguna adalah seperti berikut:</p> <p>(a) Membaca, memahami dan mematuhi Polisi Keselamatan Siber MIROS;</p> <p>(b) Mengetahui dan memahami kesan tindakannya terhadap keselamatan ICT.</p> <p>(c) Lulus tapisan keselamatan;</p> <p>(d) Melaksanakan prinsip-prinsip Polisi Keselamatan Siber MIROS;</p> <p>(e) Menjaga kerahsiaan maklumat MIROS;</p> <p>(f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;</p> <p>(g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan</p> <p>(h) Menandatangani “Surat Akuan Pematuhan” (Lampiran 1)</p>	<p style="text-align: center;">Pengguna</p>	

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 19/78

<b>020107 Jawatankuasa Keselamatan ICT (JKICT) MIROS</b>	
<p>Memandangkan MIROS bukanlah agensi yang besar, bidang kuasa jawatankuasa ini dimasukkan bersama dengan skop kuasa Jawatankuasa Pemandu ICT (JPICT) dan jawatankuasa ini juga yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MIROS.</p> <p>Keanggotaan JKICT MIROS adalah sama seperti keanggotaan ahli JPICT MIROS seperti berikut:</p> <p><b>Jawatankuasa di Peringkat MIROS</b></p> <p><b>Pengerusi</b> : Ketua Pengarah</p> <p><b>Ahli</b> : a. CDO b. ICTSO c. Pengarah Pusat d. Ketua Unit Pengurusan Kewangan dan Perolehan (KUPKP)</p> <p><b>Urus setia</b> : Ketua Unit Pengurusan Teknologi Maklumat (KUPTM)/ ICTSO</p> <p><b>Bidang kuasa:</b></p> <ul style="list-style-type: none"> <li>(a) Memperakukan/ meluluskan dokumen PKS MIROS;</li> <li>(b) Memantau tahap pematuhan keselamatan ICT;</li> <li>(c) Menilai aspek teknikal keselamatan projek-projek ICT;</li> <li>(d) Memperakukan dan meluluskan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS MIROS;</li> <li>(e) Memastikan sistem ICT sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;</li> </ul>	JPICT

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p style="text-align: right;"><b>Versi: 0.0</b></p>
		<p style="text-align: right;"><b>Muka Surat: 20/78</b></p>
<ul style="list-style-type: none"> <li>(f) Memberi nasihat kepada JPICT dari aspek keselamatan ICT;</li> <li>(g) Menilai kesesuaian teknologi untuk keperluan keselamatan ICT;</li> <li>(h) Memastikan PKS MIROS selaras dengan dasar-dasar ICT kerajaan semasa;</li> <li>(i) Membincangkan laporan keselamatan ICT dan menyelesaikan isu-isu berbangkit;</li> <li>(j) Menimbang dan meluluskan Pelan Kesinambungan Perkhidmatan (PKP) MIROS.</li> <li>(k) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan</li> <li>(l) Membincangkan pelanggaran Polisi Keselamatan Siber MIROS dan tindakan yang perlu diambil.</li> </ul>		
<p><b>020108 Pasukan Tindak Balas Insiden Keselamatan ICT MOT (CERTMOT)</b></p>		
<p>Keanggotaan CERTMOT adalah seperti berikut:</p> <p><b>Keahlian di Peringkat Kementerian</b></p> <ul style="list-style-type: none"> <li>i. <b>Pengarah</b> : CDO MOT / Pengurus IT MOT</li> <li>ii. <b>Pengurus</b> : ICTSO MOT</li> <li>iii. <b>Ahli</b> : <b>Penolong Setiausaha di BPM, MOT</b></li> <li>iv. <b>Urus setia</b>: Penolong Pegawai Teknologi Maklumat di BPM, MOT</li> </ul> <p>Memandangkan MIROS tidak mempunyai kakitangan Teknologi Maklumat yang mencukupi, CERT MIROS belum dapat diwujudkan dan sebarang insiden keselamatan ICT hendaklah dilaporkan terus kepada CERTMOT di peringkat Kementerian.</p>	<p>CERTMOT</p>	

	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 21/78

<p>Peranan dan tanggungjawab CERTMOT adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;</li> <li>(b) Merekodkan dan menjalankan siasatan awal insiden yang diterima;</li> <li>(c) Menangani tindak balas (<i>response</i>) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;</li> <li>(d) Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya;</li> <li>(e) Menasihati MOT / Jabatan mengambil tindakan pemulihan dan pengukuhan;</li> <li>(f) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna MOT / Jabatan; dan</li> <li>(g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.</li> </ul>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--


**0202 Pihak Ketiga**

**Objektif:**  
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, Pakar Runding dan lain-lain).

**020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga**


<p>Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.</p> <p>Perkara yang perlu dipatuhi termasuk yang berikut:</p> <ul style="list-style-type: none"> <li>(a) Mengenal pasti risiko keselamatan maklumat dan</li> </ul>	CDO, ICTSO, Ketua UPTM, Pentadbir Sistem ICT dan Pihak Ketiga
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------




 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 22/78


<p>kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;</p> <p>(b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna;</p> <p>(c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara yang perlu dimasukkan dalam perjanjian hendaklah selaras dengan :</p> <ul style="list-style-type: none"> <li>i. Polisi Keselamatan Siber MIROS;</li> <li>ii. Arahan Keselamatan;</li> <li>iii. Perakuan Akta Rahsia Rasmi 1972;</li> <li>iv. Hak Harta Intelek; dan</li> <li>v. Akta Perlindungan Data Peribadi 2010</li> </ul> <p>(d) Menandatangani “Surat Akuan Pematuhan” (Lampiran 1) bagi mematuhi Polisi Keselamatan Siber MIROS.</p>	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<b>BIDANG 03 - PENGURUSAN ASET ICT</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0301 Akauntabiliti Aset</b>	
<b>Objektif :</b> Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MIROS.	
<b>030101 Inventori Aset ICT</b>	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.  Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:	Pentadbir Sistem, Pegawai Aset dan semua pengguna <b>MIROS</b>

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 23/78</p>
<p>(a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;</p> <p>(b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;</p> <p>(c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MIROS;</p> <p>(d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan</p> <p>(e) Setiap pengguna adalah bertanggungjawab ke atas aset ICT di bawah kawalannya.</p>		
<p><b>0302 Pengelasan dan Pengendalian Maklumat</b></p>		
<p><b>Objektif:</b> Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.</p>		
<p><b>030201 Pengelasan Maklumat</b></p>		
<p>Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.</p> <p>Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:</p> <p>(a) Rahsia Besar;</p> <p>(b) Rahsia;</p> <p>(c) Sulit; atau</p> <p>(d) Terhad.</p>	<p>Pegawai Pengelas</p>	

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p align="center"><b>POLISI KESELAMATAN SIBER</b></p> <p align="center"><b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 24/78

<b>030202 Pengendalian Maklumat</b>	
<p>Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut :</p> <ul style="list-style-type: none"> <li>(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;</li> <li>(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;</li> <li>(c) Menentukan maklumat sedia untuk digunakan;</li> <li>(d) Menjaga kerahsiaan kata laluan;</li> <li>(e) Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;</li> <li>(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan</li> <li>(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.</li> </ul>	<p>Semua, Pegawai Pengelas</p>
<b>BIDANG 04 - PENGURUSAN OPERASI DAN KOMUNIKASI</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0401 Pengurusan Prosedur Operasi</b>	
<p><b>Objektif:</b></p> <p>Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.</p>	

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 25/78

<b>040101 Pengendalian Prosedur</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;</li> <li>(b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian <i>output</i>, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan</li> <li>(c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.</li> </ul>	Semua
<b>040102 Kawalan Perubahan</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu dan merujuk Garis Panduan Pengagihan Komputer Kepada Staf MIROS atau Garis Panduan berkaitan yang berkuatkuasa;</li> <li>(b) Aktiviti-aktiviti seperti memasang, menyelenggarakan, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;</li> <li>(c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah</li> </ul>	Semua

 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p>MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 26/78</p>

<p>ditetapkan oleh pegawai atasan atau pemilik aset ICT;</p> <p>(d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak; dan</p> <p>(e) Semua aktiviti perubahan atau pengubahsuaian hendaklah mengambil kira Garis Panduan yang sedang berkuatkuasa.</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

### 040103 Pengasingan Tugas dan Tanggungjawab

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau perubahan yang tidak dibenarkan ke atas aset ICT;</p> <p>(b) Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan</p> <p>(c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai <i>production</i>. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian jika perlu.</p>	<p>Ketua UPTM</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------

### 0402 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga


<p><b>Objektif:</b></p> <p>Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 27/78

<b>040201 Perkhidmatan Penyampaian</b>	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: <ul style="list-style-type: none"> <li>(a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga;</li> <li>(b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan</li> <li>(c) Pengurusan ke atas perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian risiko.</li> </ul>	ICTSO, UPTM
<b>0403 Perancangan dan Penerimaan Sistem</b>	
<b>Objektif :</b> Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
<b>040301 Perancangan Kapasiti</b>	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. <p>Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.</p>	Pentadbir Sistem ICT, ICTSO
<b>040302 Penerimaan Sistem</b>	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT, ICTSO

	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 28/78</p>

<p><b>0404 Perisian Berbahaya</b></p>	
<p><b>Objektif:</b></p> <p>Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, <i>trojan</i> dan sebagainya.</p>	
<p><b>040401 Perlindungan dari Perisian Berbahaya</b></p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Tidak menginstalasi (<i>uninstall</i>) sistem keselamatan yang digunakan dan telah dipasang oleh UPTM untuk mengesan perisian atau program berbahaya seperti anti virus, <i>Intrusion Detection System</i> (IDS) dan <i>Intrusion Prevention System</i> (IPS);</li> <li>(b) Memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;</li> <li>(c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya dan secara berkala;</li> <li>(d) Mengemas kini antivirus dengan <i>pattern</i> antivirus yang terkini;</li> <li>(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;</li> <li>(f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;</li> <li>(g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;</li> <li>(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan</li> </ul>	<p align="center">Semua</p>

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p align="center"><b>POLISI KESELAMATAN SIBER</b></p> <p align="center"><b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 29/78

(i) Memberi amaran dan memaklumkan mengenai ancaman keselamatan ICT seperti serangan virus.	
---------------------------------------------------------------------------------------------	--

**040402 Perlindungan dari *Mobile Code***

Penggunaan <i>mobile code</i> yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
--------------------------------------------------------------------------------------------------------	-------


**0405 Housekeeping**

<b>Objektif:</b>	
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	


**040501 *Backup***


<p>Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, <i>backup</i> seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah.</p> <p>(a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;</p> <p>(b) Membuat <i>backup</i> ke atas semua data dan maklumat mengikut keperluan operasi mengikut prosedur yang telah ditetapkan. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat;</p> <p>(c) Menguji sistem <i>backup</i> dan prosedur <i>restore</i> sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;</p> <p>(d) MIROS hendaklah menyimpan <i>backup</i> mengikut keperluan atau sekurang-kurangnya satu (1) generasi <i>backup</i>; dan</p> <p>(e) Merekodkan dan menyimpan salinan <i>backup</i> di lokasi yang berlainan dan selamat.</p>	UPTM
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------



 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 30/78

<b>0406 Pengurusan Rangkaian</b>	
<b>Objektif:</b> Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
<b>040601 Kawalan Infrastruktur Rangkaian</b>	
<p>Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Kawalan Rangkaian ini juga merangkumi Dasar Rangkaian MIROS.</p> <p>Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Semua aset rangkaian, tanggungjawab atau kerja-kerja operasi rangkaian hendaklah diasingkan untuk mengurangkan capaian. Pengubahsuaian adalah tertakluk kepada kelulusan JPICIT;</li> <li>(b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;</li> <li>(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;</li> <li>(d) <i>Firewall</i> hendaklah dipasang serta di konfigurasi dan diselia oleh Pentadbir Sistem;</li> <li>(e) Semua <i>trafik</i> keluar dan masuk hendaklah melalui <i>firewall</i> di bawah kawalan MIROS;</li> <li>(f) Semua perisian <i>sniffer</i> atau <i>network analyser</i>, <i>proxy</i> dan sebarang perisian penggadam adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;</li> </ul>	<p>UPTM / ICTSO</p>

	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
	MIROS/ITM/SPL/ICT/POL01	<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 31/78
<p>(g) Memasang perisian <i>Intrusion Prevention System</i> (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MIROS;</p> <p>(h) Memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang;</p> <p>(i) Sebarang penyambungan dan penggunaan rangkaian yang bukan di bawah kawalan MIROS adalah tidak dibenarkan kecuali dengan kebenaran khas ICTSO;</p> <p>(j) Kemudahan bagi <i>wireless</i> LAN perlu dipastikan kawalan keselamatan.</p>		
<b>0407 Pengurusan Media</b>		
<b>Objektif:</b> Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.		
<b>040701 Penghantaran dan Pemindahan</b>		
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.		Semua
<b>040702 Prosedur Pengendalian Media</b>		
Di antara prosedur-prosedur pengendalian media termasuk: <ul style="list-style-type: none"> <li>(a) Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat;</li> <li>(b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;</li> <li>(c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;</li> <li>(d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;</li> </ul>		Semua

	<p align="center"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 32/78</p>

<p>(e) Menyimpan semua media di tempat yang selamat; dan</p> <p>(f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.</p>	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

**0408 Pengurusan Pertukaran Maklumat**


**Objektif:**  
Memastikan keselamatan pertukaran maklumat dan perisian dengan agensi luar terjamin.

**040801 Pertukaran Maklumat**


<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;</p> <p>(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MIROS dengan pihak luar;</p> <p>(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MIROS;</p>	<p align="center">Semua</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------

**040802 Pengurusan Mel Elektronik (E-mel)**

<p>Penggunaan e-mel di MIROS hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan tatacara penggunaan e-mel dan Internet yang terkandung dalam Dasar Penggunaan dan Pengurusan E-mel atau Garis Panduan yang berkuatkuasa.</p>	<p align="center">Semua</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------

	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 33/78</p>

<p><b>0409 Perkhidmatan E-Dagang (<i>Electronic Commerce Services</i>)</b></p>	
<p><b>Objektif:</b></p> <p>Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.</p>	
<p><b>040901 E-Dagang</b></p>	
<p>Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;</li> <li>(b) Maklumat yang terlibat dalam transaksi dalam talian (<i>on-line</i>) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan</li> <li>(c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.</li> </ul>	<p align="center">Semua</p>
<p><b>040902 Maklumat Umum</b></p>	
<p>Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisma yang bersesuaian;</li> </ul>	<p align="center">Semua</p>

 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 34/78</p>


<p>(b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan</p> <p>(c) Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke laman web.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

**0410 Pemantauan**


**Objektif:**  
Memastikan pengesanan aktiviti pemrosesan maklumat yang tidak dibenarkan.

**041001 Pengauditan dan Forensik ICT**


<p>ICTSO mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut:</p> <p>(a) Sebarang percubaan pencerobohan kepada sistem ICT MIROS;</p> <p>(b) Serangan kod perosak (<i>malicious code</i>), halangan pemberian perkhidmatan (<i>denial of service</i>), <i>spam</i>, pemalsuan (<i>forgery, phishing</i>), pencerobohan (<i>intrusion</i>) ancaman (<i>threats</i>) dan kehilangan fizikal (<i>physical loss</i>);</p> <p>(c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;</p> <p>(d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;</p> <p>(e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;</p> <p>(f) Aktiviti instalasi dan penggunaan perisian yang membebaskan <i>bandwidth</i> rangkaian;</p> <p>(g) Aktiviti penyalahgunaan akaun e-mel; dan</p> <p>(h) Aktiviti penukaran <i>IP address</i> selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem.</p>	<p>ICTSO</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------

	<p align="center"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 35/78</p>

041002 Jejak Audit	
<p>Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekodkan aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.</p> <p>Jejak audit hendaklah mengandungi ciri-ciri berikut:</p> <ul style="list-style-type: none"> <li>(a) Rekod setiap aktiviti transaksi;</li> <li>(b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;</li> <li>(c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan</li> <li>(d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.</li> </ul> <p>Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.</p>	<p>Pentadbir Sistem ICT</p>

	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 36/78


<b>041003 Sistem Log</b>	
Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: <ul style="list-style-type: none"> <li>(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;</li> <li>(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan</li> <li>(c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO, Ketua UPTM dan CDO.</li> </ul>	Pentadbir Sistem
<b>041004 Pemantauan Log</b>	
Ianya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut: <ul style="list-style-type: none"> <li>(a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;</li> <li>(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;</li> <li>(c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;</li> <li>(d) Aktiviti pentadbiran dan operator/ pengendali sistem perlu direkodkan;</li> <li>(e) Kesalahan, kesilapan dan/ atau penyalahgunaan perlu direkod dalam log, dianalisis dan diambil tindakan sewajarnya; dan</li> </ul>	UPTM, Pentadbir Sistem

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 37/78

(f) Penyelarasan masa bagi domain keselamatan perlu menggunakan sumber masa yang sama ( <i>time synchronization</i> ).	
------------------------------------------------------------------------------------------------------------------------	--

<b>BIDANG 05 - KAWALAN CAPAIAN</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0501 Dasar Kawalan Capaian</b>	
<b>Objektif :</b> Mengawal capaian ke atas maklumat.	
<b>050101 Keperluan Kawalan Capaian</b>	
<p>Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;</li> <li>(b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;</li> <li>(c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan</li> <li>(d) Kawalan ke atas kemudahan pemprosesan maklumat.</li> </ul>	UPTM
<b>0502 Pengurusan Capaian Pengguna</b>	
<b>Objektif:</b> Mengawal capaian pengguna ke atas aset ICT.	




 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 38/78</p>


050201 Akaun Pengguna	
<p>Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> <li>(a) Akaun yang diperuntukkan oleh MIROS sahaja boleh digunakan;</li> <li>(b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;</li> <li>(c) Akaun pengguna yang diwujudkan pertama kali akan diberi hak capaian (<i>access right</i>) paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan hak capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;</li> <li>(d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MIROS. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;</li> <li>(e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan</li> <li>(f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; <ul style="list-style-type: none"> <li>i. Pengguna yang bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan;</li> <li>ii. Bertukar bidang tugas kerja;</li> <li>iii. Bertukar ke agensi lain;</li> <li>iv. Bersara; atau</li> <li>v. Ditamatkan perkhidmatan.</li> </ul> </li> </ul>	<p>Semua, Pentadbir Sistem ICT</p>

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 39/78

<b>050202 Hak Capaian</b>	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua
<b>050203 Pengurusan Kata Laluan</b>	

<p>Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MIROS seperti berikut:</p> <ul style="list-style-type: none"><li>(a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;</li><li>(b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi;</li><li>(c) Panjang kata laluan mestilah sekurang-kurangnya 13 aksara dengan gabungan aksara, angka dan aksara khusus (Alphanumeric);</li><li>(d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;</li><li>(e) Kata laluan <i>windows</i> dan <i>screen saver</i> hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;</li><li>(f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;</li><li>(g) Kuatkuasakan pertukaran kata laluan semasa <i>login</i> kali pertama atau selepas kata laluan diset semula;</li><li>(h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;</li></ul>	Semua
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
	MIROS/ITM/SPL/ICT/POL01	<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 40/78
<p>(i) Tentukan had masa <i>session</i> selama lima (5) minit (atau mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; dan</p> <p>(j) Kata laluan hendaklah ditukar selepas tempoh 120 hari atau selepas tempoh masa bersesuaian;</p>		
<b>050204 Clear Desk dan Clear Screen</b>		
<p>Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.</p> <p><i>Clear Desk</i> dan <i>Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> apabila meninggalkan komputer;</li> <li>(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan</li> <li>(c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.</li> </ul>		Semua
<b>0503 Kawalan Capaian Rangkaian</b>		
<b>Objektif:</b>		
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.		
<b>050301 Capaian Rangkaian</b>		
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:		Pentadbir Sistem ICT dan ICTSO

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 41/78</p>
<p>(a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MIROS, rangkaian agensi lain dan rangkaian awam;</p> <p>(b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan</p> <p>(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.</p>		
<p><b>050302 Capaian Internet</b></p>		

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <ul style="list-style-type: none"> <li>(a) Penggunaan Internet di MIROS hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan <i>malicious code</i>, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MIROS;</li> <li>(b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja.</li> <li>(c) Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;</li> <li>(d) Penggunaan teknologi <i>packet shaper</i> untuk mengawal aktiviti (<i>video conferencing, video streaming, chat, downloading</i>) adalah perlu bagi menguruskan penggunaan <i>bandwidth</i> yang maksimum dan lebih berkesan;</li> <li>(e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh pegawai yang diberi kuasa;</li> <li>(f) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik,</li> </ul>	<p>Pentadbir Rangkaian</p> <p>Semua</p> <p>Pentadbir Rangkaian</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 42/78

<p>rujukan sumber Internet hendaklah dinyatakan;</p> <p>(g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;</p> <p>(h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MIROS;</p> <p>(i) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali kecuali dengan kebenaran khas; dan</p> <p>(j) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:</p> <ul style="list-style-type: none"> <li>i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan</li> <li>ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan subversif.</li> </ul>	<p>Semua</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------


**050303 Capaian Jarak Jauh**


<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah <i>Remote Access</i> mestilah menggunakan kaedah penyulitan (<i>encryption</i>);</p> <p>(b) Lokasi bagi akses ke sistem ICT MIROS hendaklah dipastikan selamat; dan</p> <p>(c) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CDO / Ketua UPTM. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.</p>	<p>Semua</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------

 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p>MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 43/78</p>

<p><b>0504 Kawalan Capaian Sistem Pengoperasian</b></p>	
<p><b>Objektif:</b></p> <p>Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian</p>	
<p><b>050401 Capaian Sistem Pengoperasian</b></p>	
<p>Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan.</p> <p>Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:</p> <ul style="list-style-type: none"> <li>(a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan</li> <li>(b) Merekodkan capaian yang berjaya dan gagal.</li> </ul> <p>Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:</p> <ul style="list-style-type: none"> <li>(a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan MIROS;</li> <li>(b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf <i>super user</i>; dan</li> <li>(c) Menjana amaran (<i>alert</i>) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.</li> </ul> <p>Perkara-perkara yang perlu dipatuhi termasuk berikut:</p> <ul style="list-style-type: none"> <li>(a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur <i>log on</i> yang terjamin;</li> <li>(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap</li> </ul>	<p>Pentadbir Sistem ICT, ICTSO</p>



	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 44/78</p>
<p>pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;</p> <p>(c) Mengehadkan dan mengawal penggunaan program; dan</p> <p>(d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.</p>		
<p><b>0505 Kawalan Capaian Aplikasi dan Maklumat</b></p>		
<p><b>Objektif:</b></p> <p>Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi</p>		
<p><b>050501 Capaian Aplikasi dan Maklumat</b></p>		
<p>Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.</p> <p>Capaian sistem dan aplikasi di MIROS adalah terhad kepada pengguna dan tujuan yang dibenarkan.</p> <p>Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> <li>(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut hak capaian dan keselamatan maklumat yang telah ditentukan;</li> <li>(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);</li> <li>(c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;</li> <li>(d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan</li> </ul>	<p>Pentadbir Sistem ICT,ICTSO</p>	

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 45/78

<p>aktiviti atau capaian yang tidak sah;</p> <p>(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan</p> <p>(f) Sebarang maklumat yang perlu dimuat naik ke portal atau laman web hendaklah mendapat kebenaran daripada pegawai yang dipertanggungjawabkan.</p>	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

**0506 Peralatan Mudah Alih dan Kerja Jarak Jauh**

**Objektif:**  
Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh

**050601 Peralatan Mudah Alih**

Perkara yang perlu dipatuhi adalah seperti berikut:  (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan	Semua
-------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

**050602 Kerja Jarak Jauh**

Perkara yang perlu dipatuhi adalah seperti berikut:  (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

**BIDANG 06 : KESELAMATAN SUMBER MANUSIA**

<b>KENYATAAN</b>	<b>TINDAKAN</b>
------------------	-----------------

**0601 Keselamatan Sumber Manusia Dalam Tugas Harian**

**Objektif:**

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 46/78

pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

#### 060101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

- (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua pengguna dan pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
- (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan; dan
- (c) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan tatacara terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

Semua


UPSM

#### 060102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Memastikan semua pengguna serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan garis panduan dan peraturan serta perundangan berkaitan yang ditetapkan ;
- (b) Memberi kesedaran mengenai pengurusan keselamatan aset ICT yang berkaitan diberi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;
- (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya perlu ke atas semua pengguna,

Semua

 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 47/78</p>

<p>pembekal, pakar runding dan pihak ketiga yang berkepentingan apabila berlaku pelanggaran dengan perundangan dan peraturan ditetapkan; dan</p> <p>(d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.</p>	
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--


**060103 Bertukar Atau Tamat Perkhidmatan**

<p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <p>(a) Memastikan semua aset ICT dikembalikan kepada Pegawai Aset mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan</p> <p>(b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan.</p>	<p>Pegawai Aset, Semua</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------


**BIDANG 07 - KESELAMATAN FIZIKAL DAN PERSEKITARAN**

<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0701 Keselamatan Kawasan</b>	
<p><b>Objektif :</b></p> <p>Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.</p>	
<b>070101 Kawalan Kawasan</b>	
<p>Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.</p> <p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p>	<p>UPPF, UPTM</p>

- (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- (c) Memastikan alat penggera atau kamera sentiasa berfungsi dengan baik mengikut keperluan;
- (d) Memastikan kaunter kawalan dan perkhidmatan keselamatan diwujudkan serta mengehadkan jalan keluar masuk bagi memastikan pengguna yang dibenarkan sahaja memasuki kawasan tersebut;
- (e) Menyediakan tempat atau bilik khas untuk pelawat-pelawat;
- (f) Mereka bentuk dan melaksanakan susun atur keselamatan fizikal di dalam ruang pejabat yang mempunyai kemudahan ICT;
- (g) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana (*force majeure*);
- (h) Memastikan pihak yang dibenarkan sahaja memasuki kawasan terhad seperti kawasan penghantaran, pemunggahan dan juga lokasi lain yang dikenal pasti dari semasa ke semasa; dan
- (i) Sentiasa memastikan pihak ketiga yang membuat penyelenggaraan aset ICT diiringi.


	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 49/78

<b>070102 Kawalan Masuk Fizikal</b>	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: <ul style="list-style-type: none"> <li>(a) Semua pengguna hendaklah memakai dan mempamerkan pas keselamatan sepanjang waktu bertugas;</li> <li>(b) Pas keselamatan hendaklah dikembalikan apabila pengguna tidak lagi berkhidmat di MIROS;</li> <li>(c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter kawalan keselamatan dan hendaklah dikembalikan semula selepas tamat lawatan; dan</li> <li>(d) Kehilangan pas mestilah dilaporkan dengan kadar segera kepada pejabat yang mengeluarkannya.</li> </ul>	Semua
<b>070103 Kawasan Larangan</b>	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. <p>Perkara-perkara yang perlu dipatuhi di kawasan larangan adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan</li> <li>(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.</li> </ul>	Semua
<b>0702 Keselamatan Peralatan</b>	
<b>Objektif :</b> Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada	

	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 50/78

peralatan tersebut.	
<b>070201 Peralatan ICT</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua
<ul style="list-style-type: none"> <li>(a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;</li> <li>(b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;</li> <li>(c) Pengguna dilarang sama sekali menambah, menanggalkan atau menukar ganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran;</li> <li>(d) Pengguna dilarang membuat sebarang pemasangan (<i>installation</i>) perisian tanpa kebenaran Pentadbir Sistem atau pegawai yang dipertanggungjawabkan ;</li> <li>(e) Pengguna mestilah memastikan perisian <i>antivirus</i> di komputer mereka dikemas kini dan sentiasa melakukan imbasan ke atas media storan yang digunakan;</li> <li>(f) Semua peralatan sokongan ICT hendaklah dilindungi daripada dicuri, dirosakkan, disalah guna dan diubahsuai tanpa kebenaran;</li> <li>(g) Setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;</li> <li>(h) Peralatan-peralatan kritikal perlu dibekalkan dengan <i>Uninterruptable Power Supply</i> (UPS);</li> <li>(i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti <i>switch, hub, router</i></li> </ul>	




	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p style="text-align: right;"><b>Versi: 0.0</b></p>
		<p style="text-align: right;"><b>Muka Surat: 51/78</b></p>
<p>dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;</p> <p>(j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (<i>air ventilation</i>) yang sesuai;</p> <p>(k) Peralatan ICT yang hendak dibawa keluar dari premis agensi, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan;</p> <p>(l) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;</p> <p>(m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;</p> <p>(n) Pengguna tidak dibenarkan memindahkan peralatan ICT dari tempat asal tanpa kebenaran pegawai yang dipertanggungjawabkan;</p> <p>(o) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;</p> <p>(p) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;</p> <p>(q) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan</p> <p>(r) Pengguna hendaklah mematikan suis semua perkakasan ICT apabila meninggalkan pejabat.</p>		
<p><b>070202 Media Storan</b></p>		
<p>Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita</p>	<p style="text-align: center;">Semua</p>	

magnetik, *optical disk*, *flash disk*, CDROM dan media storan lain.

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan.

Bagi menjamin keselamatan, perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
- (b) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;
- (c) Semua data di dalam media storan yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;
- (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
- (e) Media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;
- (f) Media *backup* hendaklah diletakkan di tempat yang terkawal; dan
- (g) Membuat salinan atau penduaan (data *backup*) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.


	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
	MIROS/ITM/SPL/ICT/POL01	<b>Muka Surat:</b> 53/78


<b>070203 Media Tandatangan Digital</b>	
<p>Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah-langkah berikut:</p> <ul style="list-style-type: none"> <li>(a) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;</li> <li>(b) Media ini tidak boleh dipindah-milik atau dipinjamkan; dan</li> <li>(c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.</li> </ul>	Semua
<b>070204 Media Perisian dan Aplikasi</b>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Hanya perisian yang sah sahaja dibenarkan bagi kegunaan MIROS;</li> <li>(b) Sebarang instalasi perisian selain daripada perisian <i>pre-installed</i> oleh UPTM hendaklah mendapatkan kebenaran bertulis daripada Pengarah Pusat / Ketua Bahagian atau pegawai yang bertanggungjawab;</li> <li>(c) Sistem aplikasi dalaman tidak dibenarkan diagih/didemontasikan kepada pihak lain kecuali dengan kebenaran Ketua UPTM;</li> <li>(d) Lesen perisian (<i>registration code, serials, CD-keys</i>) perlu disimpan berasingan daripada <i>CD-ROM, disk</i> atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan</li> <li>(e) <i>Source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.</li> </ul>	Semua


	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 54/78

<b>070205 Penyelenggaraan Perkakasan</b>	
<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;</li> <li>(b) Semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi yang telah ditetapkan;</li> <li>(c) Memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja;</li> <li>(d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;</li> <li>(e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan</li> <li>(f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua UPTM atau pegawai yang bertanggungjawab.</li> </ul>	Pegawai Aset, UPTM
<b>070206 Peralatan di Luar Premis</b>	
<p>Perkakasan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan</li> <li>(b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.</li> </ul>	Semua



	<b>POLISI KESELAMATAN SIBER MIROS</b>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
	MIROS/ITM/SPL/ICT/POL01	<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 56/78
<ul style="list-style-type: none"> <li>i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti <i>RAM, Hardisk, Motherboard</i> dan sebagainya;</li> <li>ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MIROS;</li> <li>iii. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan;</li> <li>iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MIROS; dan</li> </ul> <p>(h) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau <i>thumbdrive</i> sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.</p>		
<b>0703 Keselamatan Persekitaran</b>		
<b>Objektif:</b> Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.		
<b>070301 Kawalan Persekitaran</b>		
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).  Perkara-perkara yang perlu dipatuhi adalah seperti berikut:		Semua

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p style="text-align: right;"><b>Versi: 0.0</b></p>
		<p style="text-align: right;"><b>Muka Surat: 57/78</b></p>
<ul style="list-style-type: none"> <li>(a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;</li> <li>(b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;</li> <li>(c) Peralatan perlindungan (pemadam api, pengesan kebakaran dan sebagainya) hendaklah berfungsi dan diletakkan di tempat yang bersesuaian, mudah dicapai dan dikendalikan;</li> <li>(d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;</li> <li>(e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan</li> <li>(f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer.</li> </ul>		
<p><b>070302 Bekalan Kuasa</b></p>		
<p>Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;</li> <li>(b) Peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan</li> </ul>	<p>UPTM</p>	

 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 58/78</p>

<p>(c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.</p>	
-------------------------------------------------------------------------------------------------	--

**070303 Kabel Rangkaian**

<p>Kabel rangkaian hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui <i>trunking</i> bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat;</li> <li>(b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;</li> <li>(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan <i>wire tapping</i>; dan</li> <li>(d) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.</li> </ul>	<p>UPTM</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------

**0704 Keselamatan Dokumen**

<p><b>Objektif:</b></p> <p>Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------

**070401 Dokumen**

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;</li> <li>(b) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;</li> <li>(c) Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan</li> </ul>	<p>Semua</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------



 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 59/78

Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan  (d) Menggunakan penyulitan ( <i>encryption</i> ) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

<b>BIDANG 08 - PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi</b>	
<b>Objektif :</b> Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
<b>080101 Keperluan Keselamatan Sistem Aplikasi</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;  (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan  (c) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT,ICTSO

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p align="center"><b>POLISI KESELAMATAN SIBER</b></p> <p align="center"><b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 60/78

<b>080102 Pengesahan Data Input</b>	
Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan adalah betul dan bersesuaian.	Pemilik Sistem dan Pentadbir Sistem ICT
<b>080103 Pengesahan Data Output</b>	
Data <i>output</i> daripada aplikasi perlu disahkan secara bertulis bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT
<b>0802 Kawalan Kriptografi</b>	
<b>Objektif:</b> Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
<b>080201 Penyulitan</b>	
Pengguna hendaklah membuat enkripsi ( <i>encryption</i> ) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
<b>080202 Tandatangan Digital</b>	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
<b>080303 Pengurusan Infrastruktur Kunci Awam (PKI)</b>	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
<b>0803 Keselamatan Fail Sistem</b>	
<b>Objektif:</b> Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
<b>080301 Kawalan Fail Sistem</b>	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :  (a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh	Pemilik Sistem dan Pentadbir Sistem ICT

	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 61/78

<p>pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;</p> <p>(b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;</p> <p>(c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan</p> <p>(d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.</p>	
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

#### **0804 Keselamatan Dalam Proses Pembangunan dan Sokongan**

##### **Objektif:**

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

##### **080401 Prosedur Kawalan Perubahan**

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;</p> <p>(b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi.</p> <p>(c) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;</p> <p>(d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;</p> <p>(e) Akses kepada kod sumber (source code) aplikasi perlu</p>	Pemilik Sistem dan Pentadbir Sistem ICT
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 62/78

dihadkan kepada pengguna yang diizinkan; dan  (f) Menghalang sebarang peluang untuk membocorkan maklumat.	
-----------------------------------------------------------------------------------------------------------------	--

**080402 Pembangunan Secara *Outsource***

Pembangunan perisian aplikasi secara <i>outsource</i> perlu dipantau oleh pemilik sistem.	Pemilik Sistem
-------------------------------------------------------------------------------------------	----------------

**0805 Kawalan Teknikal Keterdedahan (Vulnerability)**

<b>Objektif:</b>  Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**080501 Kawalan dari Ancaman Teknikal**


Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.  Perkara yang perlu dipatuhi adalah seperti berikut:  (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;  (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan  (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT,  ICTSO
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------

**BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN**


<b>KENYATAAN</b>	<b>TINDAKAN</b>
------------------	-----------------

**0901 Mekanisme Pelaporan Insiden Keselamatan ICT**

<b>Objektif:</b>  Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan
-----------------------------------------------------------------------------------------------------------


	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 63/78</p>

insiden keselamatan ICT.	
<b>090101 Mekanisme Pelaporan</b>	
<p>Insiden keselamatan ICT bermaksud musibah (<i>adverse event</i>) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.</p> <p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:</p> <ul style="list-style-type: none"> <li>(a) Maklumat didapati hilang, didedahkan kepada pihak –pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;</li> <li>(b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;</li> <li>(c) Kata laluan atau mekanisma kawalan akses: <ul style="list-style-type: none"> <li>i. hilang, dicuri atau didedahkan;</li> <li>ii. disyaki hilang, dicuri atau didedahkan;</li> </ul> </li> <li>(d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan</li> <li>(e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.</li> </ul> <p>Prosedur pelaporan insiden keselamatan ICT berdasarkan:</p> <ul style="list-style-type: none"> <li>(a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan</li> <li>(b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan</li> </ul>	Semua

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 64/78

Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
<b>0902 Pengurusan Maklumat Insiden Keselamatan ICT</b>	
<b>Objektif:</b> Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
<b>090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT</b>	

<p>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 MIROS.</p> <p>Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut;</p> <ul style="list-style-type: none"><li>(a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;</li><li>(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;</li><li>(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;</li><li>(d) Menyediakan tindakan pemulihan segera; dan</li><li>(e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.</li></ul>	ICTSO
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 65/78

<b>BIDANG 10 - PENGURUSAN KESINAMBUNGAN PERKHIDMATAN</b>	
<b>KENYATAAN</b>	<b>TINDAKAN</b>
<b>1001 Dasar Kesinambungan Perkhidmatan</b>	
<b>Objektif :</b> Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
<b>100101 Pelan Kesinambungan Perkhidmatan</b>	



<p>Pelan Kesenambungan Perkhidmatan (<i>Business Continuity Management</i> - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT MIROS dan perkara-perkara berikut perlu diberi perhatian:</p> <ul style="list-style-type: none"><li>(a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;</li><li>(b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;</li><li>(c) Mendokumentasikan proses dan prosedur yang telah dipersetujui;</li><li>(d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;</li><li>(e) Membuat <i>backup</i>;</li><li>(f) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau mengikut keperluan; dan</li><li>(g) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap sistem penyampaian perkhidmatan, bersama dengan kemungkinan dan impak gangguan</li></ul>	Ketua UPTM
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------



**POLISI KESELAMATAN SIBER  
MIROS**

MIROS/ITM/SPL/ICT/POL01

**Tarikh Kuat Kuasa:**

01 April 2024

**Versi: 0.0**

**Muka Surat: 66/78**

tersebut serta akibat terhadap keselamatan ICT.

Pelan Kesenambungan Perkhidmatan perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:


- (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
- (b) Senarai personal MIROS dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personal tidak dapat hadir untuk menangani insiden;
- (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;
- (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan
- (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.

Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui



 <p><b>MIROS</b> MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</p>	<p><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p>MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 68/78</p>

<p><b>1102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal</b></p>	
<p>Memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.</p> <p>Sistem ICT perlu diperiksa secara berkala bagi memastikan piawaian pelaksanaan keselamatan ICT sentiasa dipatuhi.</p>	<p>CDO, ICTSO</p>
<p><b>1103 Pematuhan Keperluan Audit</b></p>	
<p>Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem ICT.</p> <p>Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.</p> <p>Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.</p>	<p>Semua</p>
<p><b>1104 Keperluan Perundangan</b></p>	
<p>Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MIROS adalah seperti di Lampiran 3.</p>	<p>Semua</p>
<p><b>1105 Pelanggaran Dasar</b></p>	
<p>Pelanggaran Polisi Keselamatan Siber MIROS boleh dikenakan tindakan tatatertib.</p>	<p>Semua</p>

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi: 0.0</b></p>
		<p><b>Muka Surat: 69/78</b></p>

## GLOSARI

### Singkatan

CDO	Chief Digital Officer
ICT	Teknologi Maklumat & Komunikasi
ICTSO	ICT Security Officer
JKKK	Jawatankuasa Keselamatan dan Kesihatan
JPICT	Jawatankuasa Pemandu ICT
JKICT	Jawatankuasa Keselamatan ICT
KBKP	Ketua Bahagian Khidmat Pengurusan
MIROS	Institut Penyelidikan Keselamatan Jalanraya Malaysia
PKP	Pelan Kesyinambungan Perkhidmatan
UPTM	Unit Pengurusan Teknologi Maklumat
UPSM	Unit Pengurusan Sumber Manusia
UPPF	Unit Pembangunan & Pentadbiran Fasiliti

### Definisi

LAN	<p><i>Local Area Network.</i></p> <p>Rangkaian Kawasan Setempat yang menghubungkan komputer.</p>
Logout	<p><i>Log-out</i> komputer.</p> <p>Keluar daripada sesuatu sistem atau aplikasi komputer.</p>
Malicious Code	<p>Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i>, <i>worm</i>, <i>spyware</i> dan sebagainya.</p>
Mobile Code	<p>Adalah perisian yang dipindahkan di antara sistem, perisian</p>

	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 70/78</p>

dipindahkan di seluruh rangkaian dan dilaksanakan pada sistem tempatan tanpa kebenaran pemasangan oleh penerima. Contoh kod bimbit termasuk skrip ( JavaScript , VBScript ) , applet Java , kawalan ActiveX , animasi Flash , filem Shockwave ( dan Xtras ) , dan makro yang terdapat dalam dokumen Microsoft Office

**MODEM**

MOdulator DEModulator.

Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.

*Outsource*

Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

**Perisian Aplikasi**

Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.

*Public-Key Infrastructure (PKI)*

Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.

*Router*

Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

*Screen Saver*

Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.

*Server*

Pelayan komputer

*Switches*

Suis merupakan gabungan hab dan titi yang menapis

	<p style="text-align: center;"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p style="text-align: center;">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi:</b> 0.0</p>
		<p><b>Muka Surat:</b> 71/78</p>

bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.

*Threat* Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.


*Uninterruptible Power Supply (UPS)* Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

*Video Conference* Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

*Video Streaming* Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.

*Virus* Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

*Wireless LAN* Jaringan komputer yang terhubung tanpa melalui kabel.

 <small>MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH</small>	<p align="center"><b>POLISI KESELAMATAN SIBER</b></p> <p align="center"><b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 72/78

**LAMPIRAN 1**

Nama : .....

No Kad Pengenalan : .....

Jawatan : .....

Kementerian / Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya sedia maklum mengenai kewujudan Polisi Keselamatan Siber MIROS;
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber MIROS ; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

Tandatangan Pegawai

Tarikh : .....

Pengesahan Ketua Pegawai Maklumat (*Chief Digital Officer* - CDO)

.....

(Nama Pegawai Keselamatan ICT))

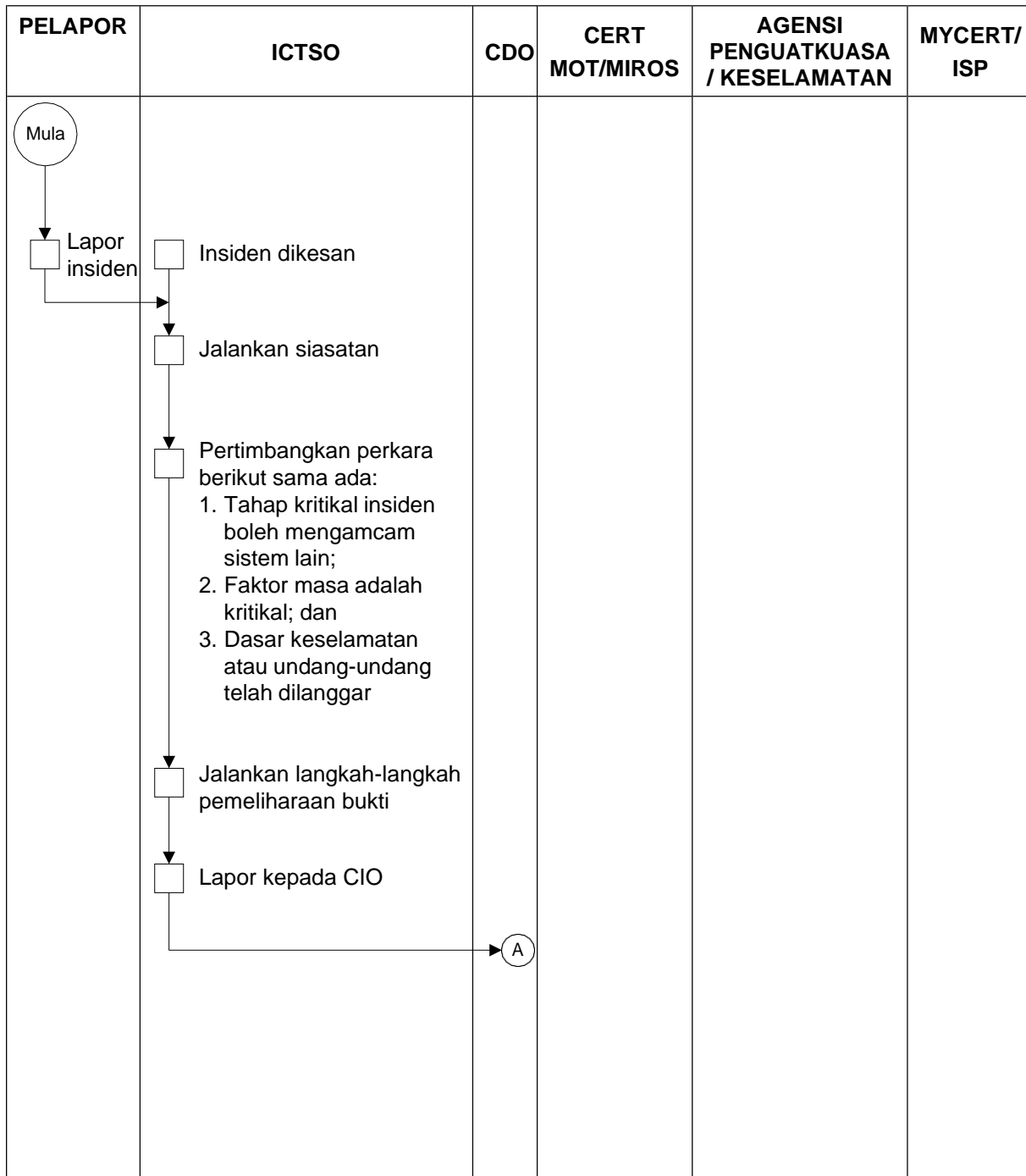
b.p Ketua Pengarah MIROS

Tarikh : .....



**LAMPIRAN 2**

**ALIR KERJA PELAPORAN INSIDEN KESELAMATAN ICT MIROS**





**POLISI KESELAMATAN SIBER  
MIROS**

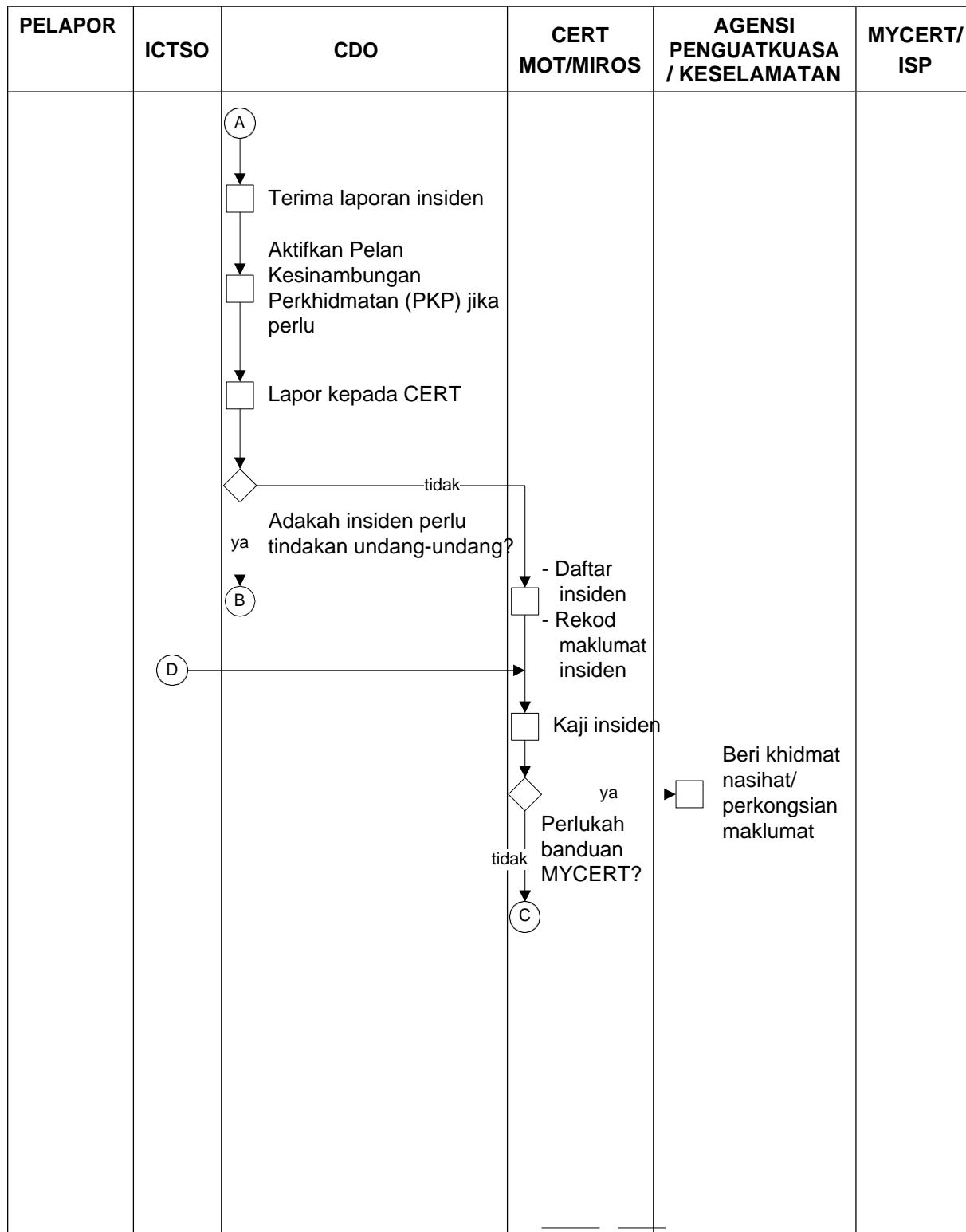
MIROS/ITM/SPL/ICT/POL01

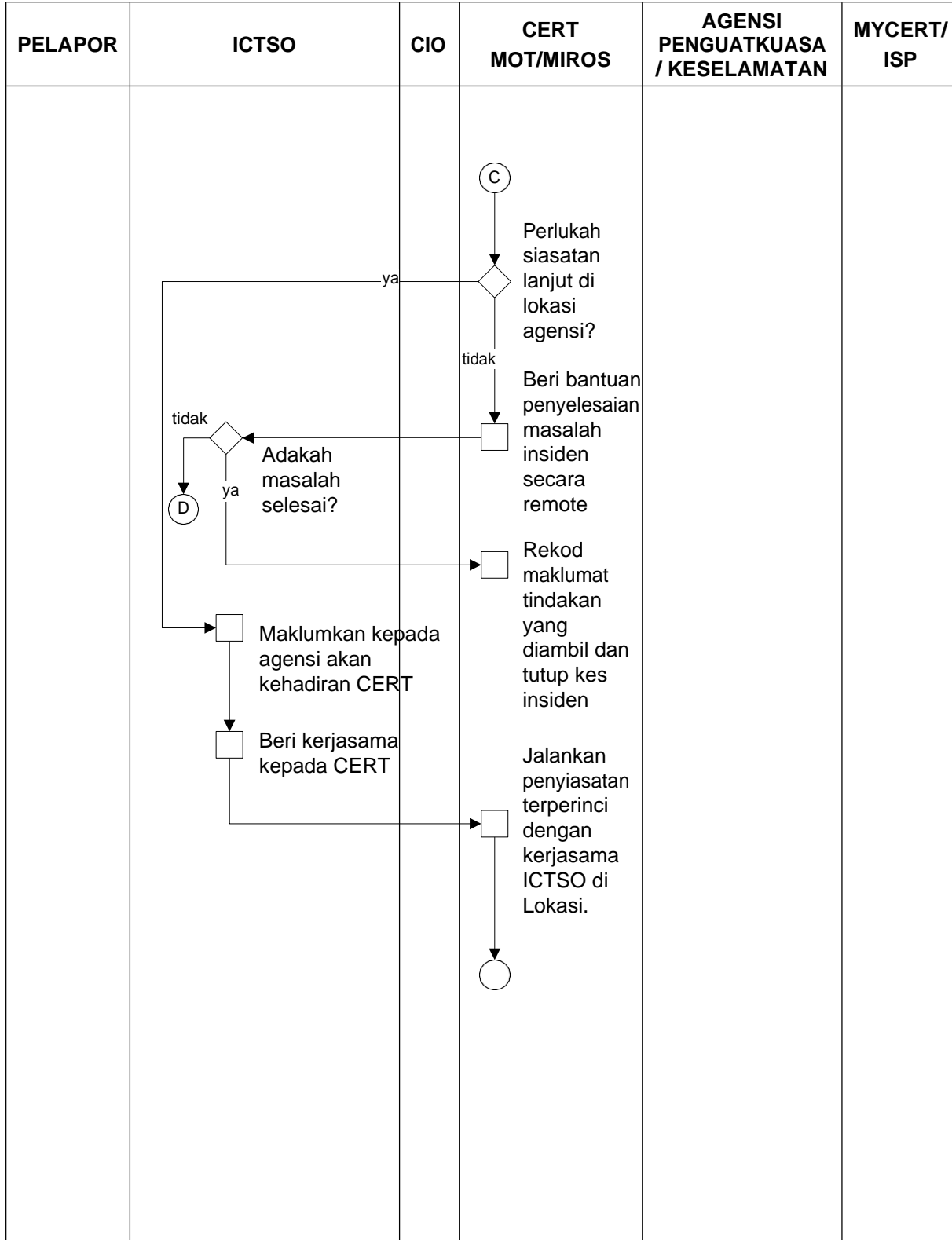
**Tarikh Kuat Kuasa:**

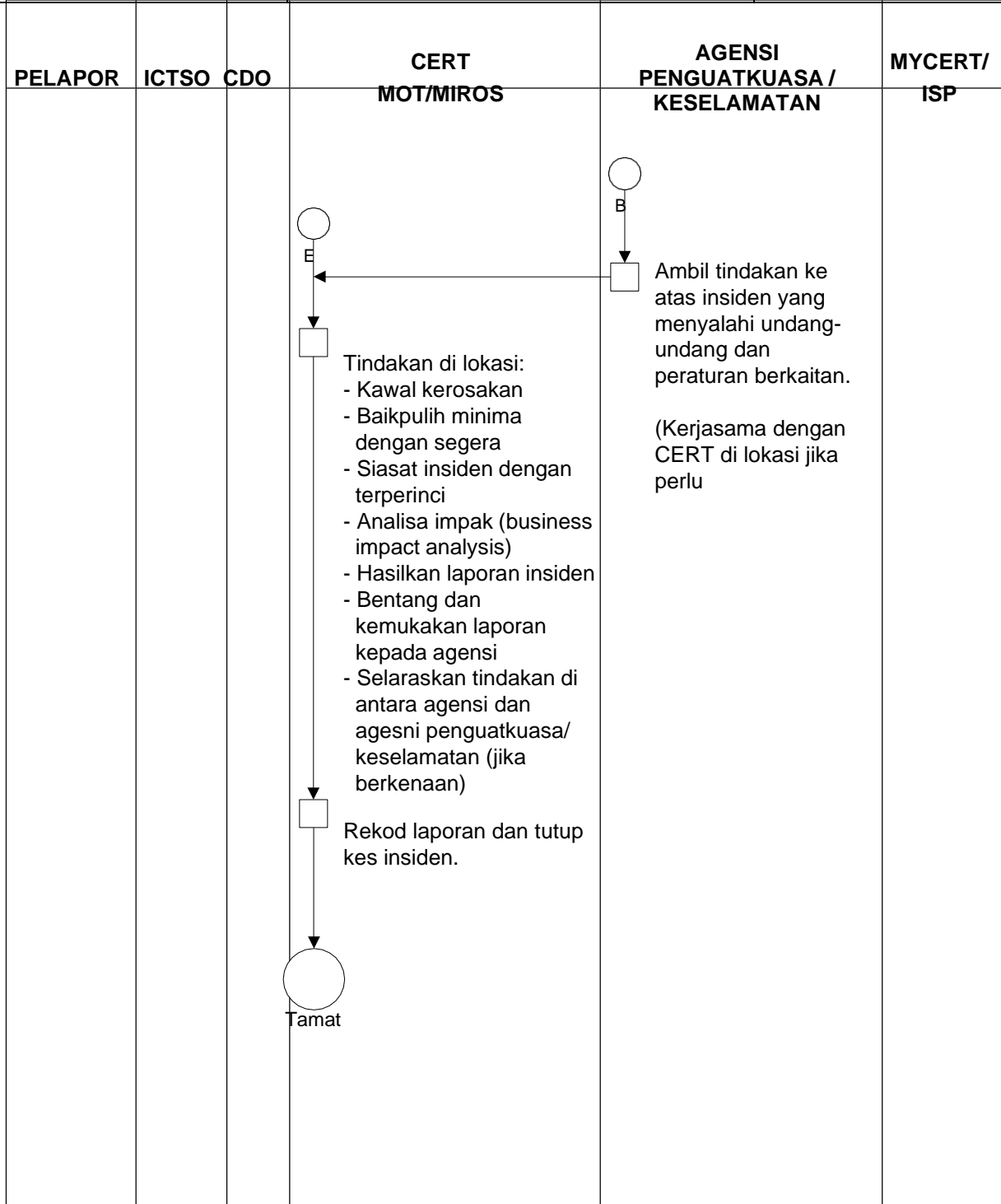
01 April 2024


**Versi: 0.0**

**Muka Surat: 74/78**







	<p align="center"><b>POLISI KESELAMATAN SIBER</b> <b>MIROS</b></p> <p align="center">MIROS/ITM/SPL/ICT/POL01</p>	<p><b>Tarikh Kuat Kuasa:</b> 01 April 2024</p>
		<p><b>Versi: 0.0</b></p>
		<p><b>Muka Surat: 77/78</b></p>

### LAMPIRAN 3

#### SENARAI PERUNDANGAN DAN PERATURAN

- (a) Arahan Keselamatan;
- (b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
- (c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
- (d) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
- (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
- (f) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- (g) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
- (h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi- Agensi Kerajaan yang bertarikh 20 Oktober 2006;
- (i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
- (j) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
- (k) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
- (l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara

Penyediaan, Penilaian dan Penerimaan Tender;

(m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan

 MALAYSIAN INSTITUTE OF ROAD SAFETY RESEARCH	<b>POLISI KESELAMATAN SIBER MIROS</b>  MIROS/ITM/SPL/ICT/POL01	<b>Tarikh Kuat Kuasa:</b> 01 April 2024
		<b>Versi:</b> 0.0
		<b>Muka Surat:</b> 78/78

Perundingan;

- (n) Akta Tandatangani Digital 1997;
- (o) Akta Rahsia Rasmi 1972;
- (p) Akta Jenayah Komputer 1997;
- (q) Akta Hak Cipta (Pindaan) Tahun 1997;
- (r) Akta Komunikasi dan Multimedia 1998;
- (s) Polisi dan SOP MIROS yang berkaitan