



KEMENTERIAN KEMAJUAN LUAR BANDAR DAN WILAYAH

# DASAR KESELAMATAN ICT

---

Versi 2.0

**23 Mac 2010**

Bahagian Pengurusan Maklumat

## KANDUNGAN

<b>Pengenalan .....</b>	<b>1</b>
<b>Objektif .....</b>	<b>1</b>
<b>Skop .....</b>	<b>1</b>
<b>Prinsip-Prinsip .....</b>	<b>1</b>
<b>PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR .....</b>	<b>4</b>
<b>Dasar Keselamatan ICT .....</b>	<b>4</b>
DKKLW-010101 Pelaksanaan Dasar .....	4
DKKLW-010102 Penyebaran Dasar .....	4
DKKLW-010103 Penyelenggaraan Dasar .....	4
DKKLW-010104 Pengecualian Dasar .....	4
<b>PERKARA 02 ORGANISASI KESELAMATAN .....</b>	<b>5</b>
<b>Infrastruktur Organisasi Keselamatan .....</b>	<b>5</b>
DKKLW-020101 Ketua Setiausaha .....	5
DKKLW-020102 Ketua Pegawai Maklumat (CIO) .....	5
DKKLW-020103 Pegawai Keselamatan ICT (ICTSO) .....	6
DKKLW-020104 Pengurus ICT .....	7
DKKLW-020105 Pentadbir Sistem ICT .....	7
DKKLW-020106 Pengguna .....	8
<b>Pihak Ketiga .....</b>	<b>9</b>
DKKLW-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga ..	9
<b>PERKARA 03 KAWALAN DAN PENGELASAN ASET .....</b>	<b>10</b>
<b>Akauntabiliti Aset .....</b>	<b>10</b>
DKKLW-030101 Inventori Aset .....	10
<b>Pengelasan dan Pengendalian Maklumat .....</b>	<b>10</b>
DKKLW-030201 Pengelasan Maklumat .....	10
DKKLW-030202 Pengendalian Maklumat .....	10



<b>Perancangan dan Penerimaan Sistem.....</b>	<b>22</b>
DKKLW-060201 Perancangan Kapasiti .....	22
DKKLW-060202 Penerimaan Sistem.....	22
<b>Perisian Berbahaya.....</b>	<b>23</b>
DKKLW-060301 Perlindungan dari Perisian Berbahaya .....	23
<b>Housekeeping.....</b>	<b>24</b>
DKKLW-060401 Penduaan .....	24
DKKLW-060402 Sistem Log.....	24
<b>Pengurusan Rangkaian.....</b>	<b>25</b>
DKKLW-060501 Kawalan Infrastruktur Rangkaian .....	25
<b>Pengurusan Media .....</b>	<b>26</b>
DKKLW-060601 Penghantaran dan Pemindahan.....	26
DKKLW-060602 Prosedur Pengendalian Media .....	26
DKKLW-060603 Keselamatan Sistem Dokumentasi .....	27
<b>PERKARA 07 KAWALAN CAPAIAN .....</b>	<b>28</b>
<b>Dasar Kawalan Capaian .....</b>	<b>28</b>
DKKLW-070101 Keperluan Kawalan Capaian.....	28
<b>Pengurusan Capaian Pengguna .....</b>	<b>29</b>
DKKLW-070201 Akaun Pengguna.....	29
DKKLW-070202 Hak Capaian.....	30
DKKLW-070203 Pengurusan Kata Laluan .....	30
DKKLW-070204 <i>Clear Desk</i> dan <i>Clear Screen</i> .....	31
<b>Kawalan Capaian Rangkaian .....</b>	<b>32</b>
DKKLW-070301 Capaian Rangkaian .....	32
DKKLW-070302 Capaian Internet .....	32
DKKLW-070303 Mel Elektronik .....	35
<b>Kawalan Capaian Sistem Pengoperasian .....</b>	<b>36</b>
DKKLW-070401 Capaian Sistem Pengoperasian .....	36
DKKLW-070402 Kad Pintar .....	37
<b>Kawalan Capaian Aplikasi dan Maklumat .....</b>	<b>38</b>
DKKLW-070501 Capaian Aplikasi dan Maklumat.....	38
<b>Peralatan Komputer Mudah Alih dan Kerja jarak Jauh.....</b>	<b>39</b>
DKKLW-070601 Peralatan Komputer Mudah Alih.....	39
DKKLW-070602 Kerja Jarak Jauh .....	40

<b>PERKARA 08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM.....</b>	<b>41</b>
<b>Keselamatan Dalam Membangunkan Sistem dan Aplikasi .....</b>	<b>41</b>
DKKLW-080101 Keperluan Keselamatan .....	41
<b>Kriptografi.....</b>	<b>41</b>
DKKLW-080201 Pengurusan Kunci .....	41
<b>Fail Sistem.....</b>	<b>42</b>
DKKLW-080301 Kawalan Sistem Fail .....	42
<b>Pembangunan dan Proses Sokongan.....</b>	<b>42</b>
DKKLW-080401 Kawalan Perubahan.....	42
<b>PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN...43</b>	
<b>Mekanisme Pelaporan .....</b>	<b>43</b>
DKKLW-090101 Mekanisme Pelaporan.....	43
DKKLW-090102 Pengurusan Maklumat Insiden Keselamatan ICT.....	44
<b>PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN .....46</b>	
<b>Dasar Kesinambungan Perkhidmatan .....</b>	<b>46</b>
DKKLW-100101 Pelan Kesinambungan Perkhidmatan.....	46
<b>PERKARA 11 PEMATUHAN .....47</b>	
<b>Pematuhan dan Keperluan Perundangan.....</b>	<b>47</b>
DKKLW-110101 Pematuhan Dasar .....	47
DKKLW-110102 Keperluan Perundangan.....	47
<b>Lampiran A .....</b>	<b>49</b>

## **PENGENALAN**

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) KKLW. Dasar ini juga menerangkan kepada semua pengguna di KKLW mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KKLW.

## **OBJEKTIF**

Dasar Keselamatan ICT KKLW diwujudkan untuk menjamin kesinambungan urusan KKLW dengan meminimumkan kesan insiden keselamatan ICT.

## **SKOP**

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan fizikal (contoh: komputer, peralatan komunikasi dan media magnet). Dasar ini adalah terpakai oleh semua pengguna di KKLW termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyediakan, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KKLW.

## **PRINSIP-PRINSIP**

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KKLW 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 (*read-only*). Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

**c. Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT KKLW;

**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 terperinci atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan 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*;

**f. Pematuhan**

Dasar Keselamatan ICT KKLW 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.

**Perkara 01 Pembangunan dan Penyelenggaraan Dasar**

<b>Dasar Keselamatan ICT</b>		
<b>DKKLW-010101 Pelaksanaan Dasar</b>		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha KKLW dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan semua Setiausaha Bahagian.	Ketua Setiausaha
<b>DKKLW-010102 Penyebaran Dasar</b>		
	Dasar ini perlu disebarikan kepada semua pengguna KKLW (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
<b>DKKLW-010103 Penyelenggaraan Dasar</b>		
	Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT KKLW: <ul style="list-style-type: none"> <li>a. kenal pasti dan tentukan perubahan yang diperlukan;</li> <li>b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT);</li> <li>c. perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan</li> <li>d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.</li> </ul>	ICTSO
<b>DKKLW-010104 Pengecualian Dasar</b>		
	Dasar Keselamatan ICT KKLW adalah terpakai kepada semua pengguna ICT KKLW dan tiada pengecualian diberikan.	Semua

**Perkara 02 Organisasi Keselamatan**

<b>Infrastruktur Organisasi Keselamatan</b>		
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
<b>DKKLW-020101 Ketua Setiausaha</b>		
	<p>Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KKLW;</li> <li>b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT KKLW;</li> <li>c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan</li> <li>d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KKLW.</li> </ul>	Ketua Setiausaha
<b>DKKLW-020102 Ketua Pegawai Maklumat (CIO)</b>		
	<p>Setiausaha Bahagian Kanan (Khidmat Pengurusan) KKLW adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab beliau adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>a. membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;</li> <li>b. menentukan keperluan keselamatan ICT; dan</li> <li>c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.</li> </ul>	CIO

<b>DKKLW-020103 Pegawai Keselamatan ICT (ICTSO)</b>	
	<p>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>a. mengurus keseluruhan program-program keselamatan ICT KKLW;</li> <li>b. menguatkuasakan Dasar Keselamatan ICT KKLW;</li> <li>c. Memastikan semua pengguna memahami dan mematuhi Dasar Keselamatan ICT;</li> <li>d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KKLW;</li> <li>c. menjalankan pengurusan risiko;</li> <li>d. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;</li> <li>e. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;</li> <li>f. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) KKLW dan memaklumpkannya kepada CIO;</li> <li>g. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkahbaik pulih dengan segera;</li> <li>h. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KKLW; dan</li> <li>i. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.</li> </ul>

<b>DKKLW-020104 Pengurus ICT</b>		
	<p>Setiausaha Bahagian ICT merupakan Pengurus ICT yang memainkan peranan dan tanggungjawab seperti berikut:</p> <ol style="list-style-type: none"> <li>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT KKLW;</li> <li>b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KKLW;</li> <li>c. menentukan kawalan akses semua pengguna terhadap aset ICT KKLW;</li> <li>d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan</li> <li>e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KKLW.</li> </ol>	Pengurus ICT
<b>DKKLW-020105 Pentadbir Sistem ICT</b>		
	<p>Pegawai Teknologi Maklumat Bahagian ICT, KKLW adalah merupakan Pentadbir Sistem ICT KKLW. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:</p> <ol style="list-style-type: none"> <li>a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;</li> <li>b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KKLW;</li> <li>c. memantau aktiviti capaian harian pengguna;</li> <li>d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta;</li> </ol>	Bahagian ICT

	<p>e. menyimpan dan menganalisis rekod jejak audit; dan</p> <p>f. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.</p>	
<p><b>DKKLW-020106 Pengguna</b></p>		
	<p>Peranan dan tanggungjawab pengguna adalah seperti berikut:</p> <p>a. membaca, memahami dan mematuhi Dasar Keselamatan ICT KKLW;</p> <p>b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;</p> <p>c. lulus tapisan keselamatan;</p> <p>d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat KKLW;</p> <p>e. melaksanakan langkah-langkah perlindungan seperti berikut :-</p> <ol style="list-style-type: none"> <li>1. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;</li> <li>2. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;</li> <li>3. menentukan maklumat sedia untuk digunakan;</li> <li>4. menjaga kerahsiaan kata laluan;</li> <li>5. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;</li> <li>6. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan</li> <li>7. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.</li> </ol> <p>f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO</p>	<p>Pengguna</p>

	<p>dengan segera;</p> <p>g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan</p> <p>h. menandatangani surat akuan pematuhan Dasar Keselamatan ICT KKLW.</p>	
<b>Pihak Ketiga</b>		
<p>Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.</p>		
<b>DKKLW-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga</b>		
	<p>Akses kepada aset ICT KKLW perlu berlandaskan kepada perjanjian kontrak.</p> <p>Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan.</p> <ul style="list-style-type: none"> <li>a. Dasar Keselamatan ICT KKLW;</li> <li>b. Tapisan Keselamatan;</li> <li>c. Perakuan Akta Rahsia Rasmi 1972;</li> <li>d. Hak Harta Intelek;</li> </ul> <p>Nota 1:</p> <p>Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan juga boleh dirujuk.</p>	<p>CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga</p>



	<ul style="list-style-type: none"><li>c. menentukan maklumat sedia untuk digunakan;</li><li>d. menjaga kerahsiaan kata laluan;</li><li>e. mematuhi standard, 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 kerahsian langkah-langkah keselamatan ICT dari diketahui umum.</li></ul>	
--	--	--

**Perkara 04 Keselamatan Sumber Manusia**

<b>Keselamatan ICT Dalam Tugas Harian</b>		
Objektif: Meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT KKLW.		
<b>DKKLW-040101 Tanggungjawab Keselamatan</b>		
	<p>Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.</p> <p>Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.</p>	Semua
<b>DKKLW-040102 Terma dan Syarat Perkhidmatan</b>		
	Semua warga KKLW yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
<b>DKKLW-040103 Perakuan Akta Rahsia Rasmi</b>		
	Warga KKLW yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
<b>Menangani Insiden Keselamatan ICT</b>		
Objektif: Meminimumkan kesan insiden keselamatan ICT.		
<b>DKKLW-040201 Pelaporan Insiden</b>		
	<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</li> </ul>	Semua

	<p>kebenaran atau disyaki sedemikian;</p> <p>c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;</p> <p>d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;</p> <p>e. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini.</p> <p>Nota 2:</p> <p>Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk.</p>	
<b>Pendidikan</b>		
<p>Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.</p>		
<b>DKKLW-040301 Program Kesedaran Keselamatan ICT</b>		
	<p>Setiap pengguna di KKLW perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.</p> <p>Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT KKLW.</p>	ICTSO
<b>Tindakan Tatatertib</b>		
<p>Objektif: Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT KKLW.</p>		
<b>DKKLW-040401 Pelanggaran Dasar</b>		
	<p>Pelanggaran Dasar Keselamatan ICT KKLW akan dikenakan tindakan tatatertib.</p>	Semua

**Perkara 05 Keselamatan Fizikal**

<b>Keselamatan Kawasan</b>		
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.		
<b>DKKLW-050101 Perimeter Keselamatan Fizikal</b>		
	<p>Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk mencero boh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut :</p> <ol style="list-style-type: none"> <li>a. Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;</li> <li>b. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;</li> <li>c. Memperkukuhkan dinding dan siling;</li> <li>d. Memasang alat penggera atau kamera;</li> <li>e. Menghadkan jalan keluar masuk;</li> <li>f. Mengadakan kaunter kawalan;</li> <li>g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan</li> <li>h. Mewujudkan perkhidmatan kawalan keselamatan.</li> </ol>	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO
<b>DKKLW-050102 Kawalan Masuk Fizikal</b>		
	<ol style="list-style-type: none"> <li>a. Setiap pengguna KKLW hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;</li> <li>b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan;</li> </ol>	Semua dan pelawat

	<p>c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara;</p> <p>d. Setiap pelawat hendaklah mendaftar di Kaunter Pelawat Blok D9 terlebih dahulu;</p> <p>e. Kehilangan pas mestilah dilaporkan dengan segera;</p> <p>f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT KKLW;</p>	
<p><b>DKKLW-050103 Kawasan Larangan</b></p>		
	<p>Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut :</p> <p>a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu.</p> <p>b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan</p> <p>c. Semua penggunaan peralatan yang melibatkan penghantaran, kemas kinidan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.</p>	<p>Semua</p>
<p><b>Keselamatan Peralatan</b></p>		
<p>Objektif: Melindung peralatan dan maklumat.</p>		
<p><b>DKKLW-050201 Perkakasan</b></p>		
	<p>Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh</p>	<p>Semua</p>

	<p>digunakan bila perlu:</p> <ol style="list-style-type: none"> <li>a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;</li> <li>b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;</li> <li>c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan</li> <li>d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.</li> </ol>	
<b>DKKLW-050202 Dokumen</b>		
	<p>Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> <li>a. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;</li> <li>b. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;</li> <li>c. menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan</li> <li>d. memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.</li> </ol>	Semua
<b>DKKLW-050203 Media Storan</b>		
	<p>Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat :</p>	Semua

	<ul style="list-style-type: none"> <li>a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;</li> <li>b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;</li> <li>c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan</li> <li>d. Pergerakan media storan hendaklah direkodkan.</li> </ul>	
<p><b>DKKLW-050204 Kabel</b></p>		
	<p>Kabel komputer hendaklah di lindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :</p> <ul style="list-style-type: none"> <li>a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;</li> <li>b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan</li> <li>c. Melindung laluan pemasangan kabel sepenuhnya.</li> </ul>	<p>Bahagian ICT dan ICTSO</p>
<p><b>DKKLW-050205 Penyelenggaraan</b></p>		
	<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.</p> <ul style="list-style-type: none"> <li>a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;</li> <li>b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;</li> <li>c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan</li> </ul>	<p>Semua</p>

	d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah Bahagian berkenaan.	
<b>DKKLW-050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat</b>		
	<p>Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan :</p> <p>a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan</p> <p>b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.</p>	Semua
<b>DKKLW-050207 Peralatan di Luar Premis</b>		
	<p>Bagi perkakasan yang dibawa keluar dari premis KKLW, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan KKLW:</p> <p>a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan</p> <p>b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.</p>	Semua
<b>DKKLW-050208 Pelupusan</b>		
	<p>Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KKLW:</p> <p>a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui <i>shredding, grinding, degauzing</i> atau pembakaran;</p>	Semua

	<p>b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan</p> <p>c. Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".</p>	
<p><b>DKKLW-050209 Clear Desk dan Clear Screen</b></p>		
	<p>Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. <i>Clear Desk</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya :</p> <p>a. Gunakan kemudahan <i>password screen saver</i> atau log keluar apabila meninggalkan komputer;</p> <p>b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan</p>	<p>Semua</p>
<p><b>Keselamatan Persekitaran</b></p>		
<p>Objektif: Melindungi aset ICT KKLW dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.</p>		
<p><b>DKKLW-050301 Kawalan Persekitaran</b></p>		
	<p>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). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil :</p> <p>a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;</p> <p>b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah</p>	<p>Semua</p>

	<p>dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;</p> <p>c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;</p> <p>d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;</p> <p>e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;</p> <p>f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan</p> <p>g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.</p>	
<p><b>DKKLW-050302 Bekalan Kuasa</b></p>		
	<p>a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;</p> <p>b. Peralatan sokongan seperti UPS (<i>Uninterruptable Power Supply</i>) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan;</p> <p>c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.</p>	<p>Bahagian ICT, ICTSO</p>
<p><b>DKKLW-050303 Prosedur Kecemasan</b></p>		
	<p>a. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik;</p>	<p>Semua</p>

**Perkara 06 Pengurusan Operasi dan Komunikasi**

<b>Pengurusan Prosedur Operasi</b>		
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.		
<b>DKKLW-060101 Pengendalian Prosedur</b>		
	<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 output, 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>DKKLW-060102 Kawalan Perubahan</b>		
	<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;</li> <li>b. Aktiviti-aktiviti seperti memasang, menyelenggara, 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 ditetapkan; dan</li> <li>d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.</li> </ul>	Semua

<b>DKKLW-060103 Prosedur Pengurusan Insiden</b>		
	<p>Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut:</p> <ul style="list-style-type: none"> <li>a. mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;</li> <li>b. menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;</li> <li>c. menyimpan jejak audit dan memelihara bahan bukti; dan</li> <li>d. menyediakan tindakan pemulihan segera.</li> </ul>	JPICT KKLW , ICTSO
<b>Perancangan dan Penerimaan Sistem</b>		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
<b>DKKLW-060201 Perancangan Kapasiti</b>		
	<ul style="list-style-type: none"> <li>a. 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; dan</li> <li>b. 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.</li> </ul>	Pentadbir Sistem ICT, ICTSO
<b>DKKLW-060202 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

<b>Perisian Berbahaya</b>		
<p>Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.</p>		
<p><b>DKKLW-060301 Perlindungan dari Perisian Berbahaya</b></p>		
	<ul style="list-style-type: none"> <li>a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan <i>Intrusion Detection System</i> (IDS) dan mengikut prosedur penggunaan yang betul dan selamat;</li> <li>b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;</li> <li>c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;</li> <li>d. Mengemas kini <i>pattern</i> anti virus setiap masa;</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> <li>i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.</li> </ul>	<p>Semua</p>

<b>Housekeeping</b>		
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.		
<b>DKKLW-060401 Penduaan</b>		
	<p>Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di <i>off site</i>.</p> <ol style="list-style-type: none"> <li>a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;</li> <li>b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan</li> <li>c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.</li> </ol>	Semua
<b>DKKLW-060402 Sistem Log</b>		
	<ol 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 tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.</li> </ol>	Bahagian ICT

<b>Pengurusan Rangkaian</b>	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
<b>DKKLW-060501 Kawalan Infrastruktur Rangkaian</b>	
<p>Infrastruktur Rangkaian mestilah di kawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :-</p> <ol style="list-style-type: none"> <li>a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;</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. Semua peralatan mestilah melalui proses <i>Factory Acceptance Check</i> (FAC) semasa pemasangan dan konfigurasi;</li> <li>e. <i>Firewall</i> hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem;</li> <li>f. Semua trafik keluar dan masuk hendaklah melalui <i>firewall</i> di bawah kawalan KKLW;</li> <li>g. Semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;</li> <li>h. Memasang perisian <i>Intrusion Detection System</i> (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KKLW;</li> <li>i. Memasang <i>Web Content Filter</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling</li> </ol>	Bahagian ICT

	<p>Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";</p> <p>j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KKLW hendaklah mendapat kebenaran ICTSO;</p> <p>k. Semua pengguna hanya dibenarkan menggunakan rangkaian KKLW sahaja. Penggunaan modem adalah dilarangsama sekali; dan</p> <p>l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.</p>	
<b>Pengurusan Media</b>		
<p>Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.</p>		
<b>DKKLW-060601 Penghantaran dan Pemindahan</b>		
	<p>Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.</p>	<p>Semua</p>
<b>DKKLW-060602 Prosedur Pengendalian Media</b>		
	<p>a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;</p> <p>b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja;</p> <p>c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan;</p> <p>d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahanyang tidak dibenarkan;</p> <p>e. Menyimpan semua media di tempat yang selamat; dan</p> <p>f. Media yang mengandungi maklumat rahsia</p>	<p>Semua</p>

	<p>rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.</p>	
<p><b>DKKLW-060603 Keselamatan Sistem Dokumentasi</b></p>		
	<ul style="list-style-type: none"> <li>a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;</li> <li>b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan</li> <li>c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.</li> </ul>	<p>Pentadbir Sistem ICT, ICTSO</p>

**Perkara 07 Kawalan Capaian**

<b>DKKKLW-0701 Dasar Kawalan Capaian</b>	
<b>Objektif:</b> Mengawal capaian ke atas maklumat.	
<b>DKKKLW-070101 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 dikajisemula berasaskan keperluan perkhidmatan dan keselamatan.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;</p> <p>(b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;</p> <p>(c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan</p> <p>(d) Kawalan ke atas kemudahan pemprosesan maklumat.</p>	<p>Bahagian Pengurusan Maklumat dan ICTSO</p>

<b>DKKKLW-0702 Pengurusan Capaian Pengguna</b>	
<b>Objektif:</b> Mengawal capaian pengguna ke atas aset ICT KKLW.	
<b>DKKKLW-070201 Akaun Pengguna</b>	
<p>Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.</p> <p>Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:</p> <p>(a) Akaun yang diperuntukkan oleh KKLW sahaja boleh digunakan;</p> <p>(b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;</p> <p>(c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;</p> <p>(d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KKLW. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;</p> <p>(e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan</p> <p>(f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:</p> <p>i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu;</p>	<p>Semua dan Pentadbir Sistem ICT</p>

<ul style="list-style-type: none"> <li>ii. Bertukar bidang tugas kerja;</li> <li>iii. Bertukar ke agensi lain;</li> <li>iv. Akaun e-mel penuh;</li> <li>v. Bersara; atau</li> <li>vi. Ditamatkan perkhidmatan.</li> </ul>	
<p><b>DKKKLW-070202 Hak Capaian</b></p>	
<p>Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.</p>	<p>Pentadbir Sistem ICT</p>
<p><b>DKKKLW-070203 Pengurusan Kata Laluan</b></p>	
<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 KKLW 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 dikompromi;</li> <li>(c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus;</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> </ul>	<p>Semua dan Pentadbir Sistem ICT</p>

<p>(f) Kata laluan hendaklah tidak dipaparkan semasa <i>input</i>, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;</p> <p>(g) Kuatkuasakan pertukaran kata laluan semasa <i>login</i> kali pertama atau selepas <i>login</i> kali pertama atau selepas kata laluan diset semula;</p> <p>(h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;</p> <p>(i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;</p> <p>(j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan</p> <p>(k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.</p>	
<p><b>DKKKLW-070204    <i>Clear Desk dan Clear Screen</i></b></p>	
<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 dan 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> <p>(a) Menggunakan kemudahan <i>password screen saver</i> atau <i>logout</i> apabila meninggalkan komputer;</p> <p>(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan</p>	<p>Semua</p>

<p>(c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.</p>	
<p><b>DKKKLW-0703 Kawalan Capaian Rangkaian</b></p>	
<p><b>Objektif:</b> Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.</p>	
<p><b>DKKKLW-070301 Capaian Rangkaian</b></p>	
<p>Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:</p> <p>(a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KKLW, 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>Pentadbir Sistem ICT dan ICTSO</p>
<p><b>DKKKLW-070302 Capaian Internet</b></p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Penggunaan Internet di KKLW 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</p>	<p>Pentadbir Rangkaian</p>

<p>dalam rangkaian KKLW;</p> <p>(b) Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;</p> <p>(c) Penggunaan teknologi (<i>packet shaper</i>) untuk mengawal aktiviti (<i>video conferencing, video streaming, chat, downloading</i>) adalah perlu bagi menguruskan penggunaan jalur lebar (<i>bandwidth</i>) yang maksimum dan lebih berkesan;</p> <p>(d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;</p> <p>(e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa;</p> <p>(f) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;</p> <p>(g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet;</p> <p>(h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;</p> <p>(i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KKLW;</p> <p>(j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti <i>newsgroup</i> dan <i>bulletin board</i>. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu</p>	<p>Pengurus ICT</p> <p>Semua</p>
---	----------------------------------

tertakluk kepada dasar dan peraturan yang telah ditetapkan;

(k) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

(l) Pengguna adalah dilarang melakukan sebarang aktiviti yang melanggar tatacara penggunaan internet seperti berikut:

(a) memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen;

(b) menyedia dan menghantar maklumat berulang-ulang berupa gangguan;

(c) menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah;

(d) menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan;

(e) menyalahgunakan kemudahan perbincangan awam atas talian seperti *newsgroup* dan *bulletin board*;

(f) memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;

(g) memuat turun, memuat naik, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu; dan

<p>(h) menggunakan kemudahan <i>chatting</i> melalui Internet;</p>	
<p><b>DKKLW-070303 Mel Elektronik</b></p>	
<p>a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KKLW sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;</p> <p>b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KKLW;</p> <p>c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;</p> <p>d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;</p> <p>e. Pengguna dinasihatkan menggunakan fail keipilan, sekiranya perlu. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;</p> <p>f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;</p> <p>g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;</p> <p>h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;</p>	<p>Semua</p>

<p>i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi perlulah dihapuskan;</p> <p>j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan</p> <p>k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".</p>	
--	--

**DKKKLW-0704 Kawalan Capaian Sistem Pengoperasian**

**Objektif:**  
 Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

**DKKKLW-070401 Capaian Sistem Pengoperasian**

<p>Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer.</p> <p>Kemudahan ini juga perlu bagi:</p> <p>(a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan</p> <p>(b) Merekodkan capaian yang berjaya dan gagal.</p> <p>Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-erkara berikut:</p>	<p>Pentadbir Sistem ICT dan ICTSO</p>
--	---------------------------------------

<p>(a) Mengesahkan pengguna yang dibenarkan;</p> <p>(b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf <i>super user</i>; dan</p> <p>(c) Menjana amaran (<i>alert</i>) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur <i>log on</i> yang terjamin;</p> <p>(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;</p> <p>(c) Menghadkan dan mengawal penggunaan program; dan</p> <p>(d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.</p>	
<p><b>DKKKLW-070402 Kad Pintar</b></p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;</p> <p>(b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;</p> <p>(c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan</p>	<p>Semua</p>

<p>sebanyak tiga (3) kali cubaan akan disekat; dan</p> <p>(d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Pengurusan Maklumat, KKLW.</p>	
<p><b>DKKKLW-0705 Kawalan Capaian Aplikasi dan Maklumat</b></p>	
<p><b>Objektif:</b> Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi</p>	
<p><b>DKKKLW-070501 Capaian Aplikasi dan Maklumat</b></p>	
<p>Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, Perkara-perkara berikut hendaklah dipatuhi:</p> <p>(a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;</p> <p>(b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna</p>	<p>Pentadbir Sistem ICT dan ICTSO</p>

<p>hendaklah direkodkan (sistem log);</p> <p>(c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;</p> <p>(d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan</p> <p>(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.</p>	
<p><b>DKKKLW-0706 Peralatan Mudah Alih dan Kerja Jarak Jauh</b></p>	
<p><b>Objektif:</b> Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh</p>	
<p><b>DKKKLW-070601 Peralatan Mudah Alih</b></p>	
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.</p>	<p>Semua</p>

<b>DKKKLW-070602 Kerja Jarak Jauh</b>	
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

**Perkara 08 Pembangunan dan Penyelenggaraan Sistem**

<b>Keselamatan Dalam Membangunkan Sistem dan Aplikasi</b>		
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
<b>DKKLW-080101 Keperluan Keselamatan</b>		
	<p>a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;</p> <p>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</p> <p>c. Sebaiknya-baiknya, 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.</p>	Pemilik sistem, Pentadbir Sistem ICT, ICTSO
<b>Kriptografi</b>		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
<b>DKKLW-080201 Pengurusan Kunci</b>		
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

<b>Fail Sistem</b>		
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
<b>DKKLW-080301 Kawalan Fail Sistem</b>		
	<ul style="list-style-type: none"> <li>a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;</li> <li>b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;</li> <li>c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan</li> <li>d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan.</li> </ul>	Pentadbir Sistem ICT
<b>Pembangunan dan Proses Sokongan</b>		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
<b>DKKLW-080401 Kawalan Perubahan</b>		
	Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem ICT

**Perkara 09 Pengurusan Pengendalian Insiden Keselamatan**

<b>DKKKLW-0901 Mekanisme Pelaporan Insiden Keselamatan ICT</b>	
<b>Objektif:</b> Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
<b>DKKKLW-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. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT KKLW dengan kadar segera:</p> <p>(a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;</p> <p>(b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;</p> <p>(c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;</p> <p>(d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan</p> <p>(e) Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak dijangka.</p> <p>Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan</p>	<p>Semua</p>

<p>insiden keselamatan ICT di KKLW sepertimana Lampiran A. Prosedur pelaporan insiden keselamatan ICT berdasarkan:</p> <p>(a) Pekeliling Am Bilangan 1 Tahun 2001 -Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan</p> <p>(b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.</p>	
<p><b>DKKKLW-0902 Pengurusan Maklumat Insiden Keselamatan ICT</b></p>	
<p><b>Objektif:</b> Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.</p>	
<p><b>DKKKLW-090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT</b></p>	
<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 KKLW. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggara. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:</p> <p>(a) Menyimpan jejak audit, <i>backup</i> secara berkala dan melindungi integriti semua bahan bukti;</p> <p>(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;</p>	<p>ICTSO</p>

<p>(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;</p> <p>(d) Menyedia tindakan pemulihan segera; dan</p> <p>(e) Memaklum atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.</p>	
---	--

**Perkara 10 Pengurusan Kesenambungan Perkhidmatan**

<b>Dasar Kesenambungan Perkhidmatan</b>		
<p>Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.</p>		
<b>DKKLW-100101 Pelan Kesenambungan Perkhidmatan</b>		
	<p>Pelan kesinambungan perkhidmatan 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 dan perkara-perkara berikut perlu diberi perhatian:</p> <ol 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 penduaan; dan</li> <li>f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.</li> </ol>	ICTSO

**Perkara 11 Pematuhan**

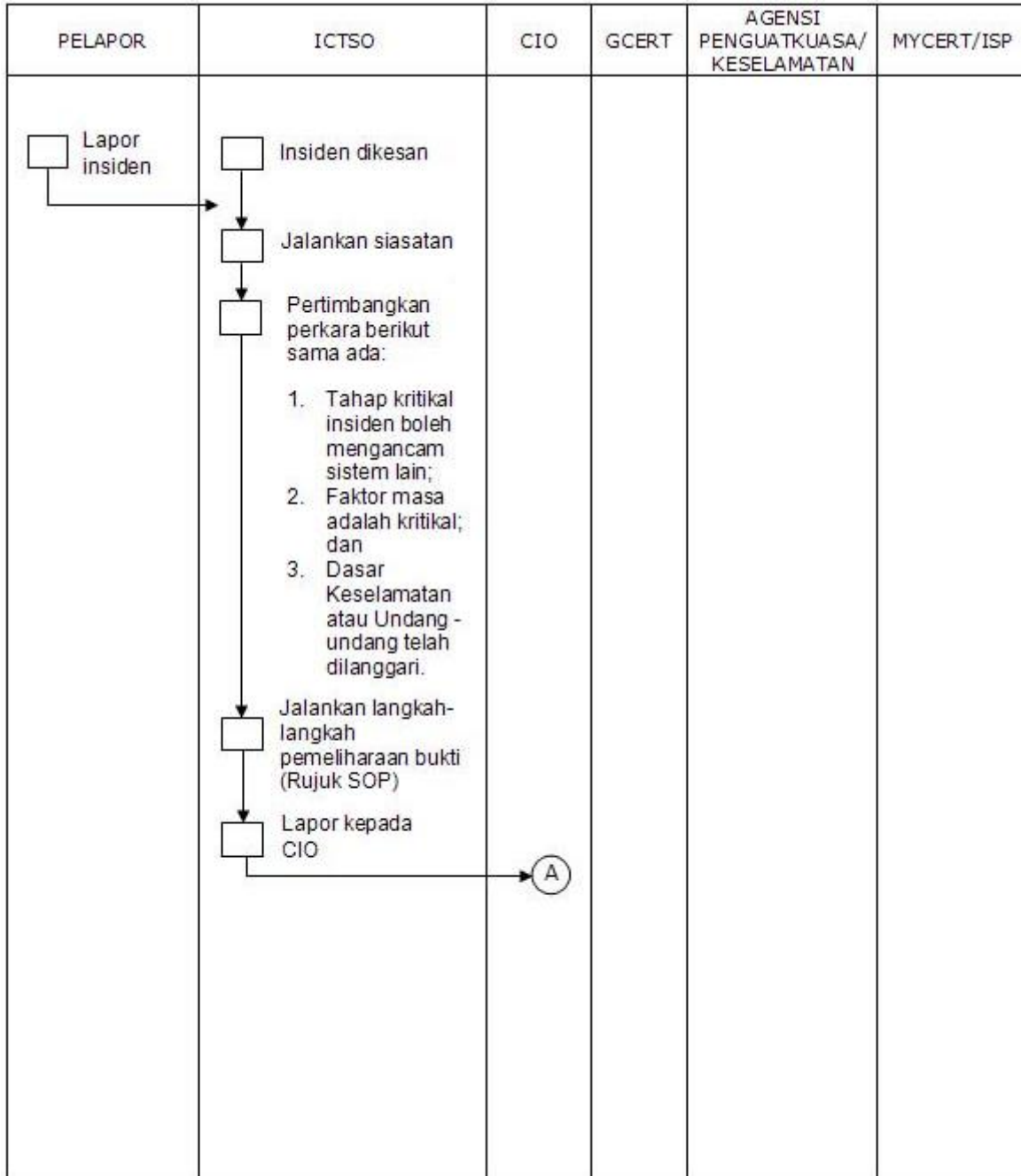
<b>Pematuhan dan Keperluan Perundangan</b>		
<p>Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT KKLW.</p>		
<b>DKKLW-110101 Pematuhan Dasar</b>		
	<p>Setiap pengguna di KKLW hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT KKLW dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.</p> <p>Semua aset ICT di KKLW termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.</p>	Semua
<b>DKKLW-110102 Keperluan Perundangan</b>		
	<p>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KKLW:</p> <ol style="list-style-type: none"> <li>a. Arahan Keselamatan;</li> <li>b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";</li> <li>c. <i>Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)</i>;</li> <li>d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)</li> <li>e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";</li> <li>f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;</li> </ol>	Semua

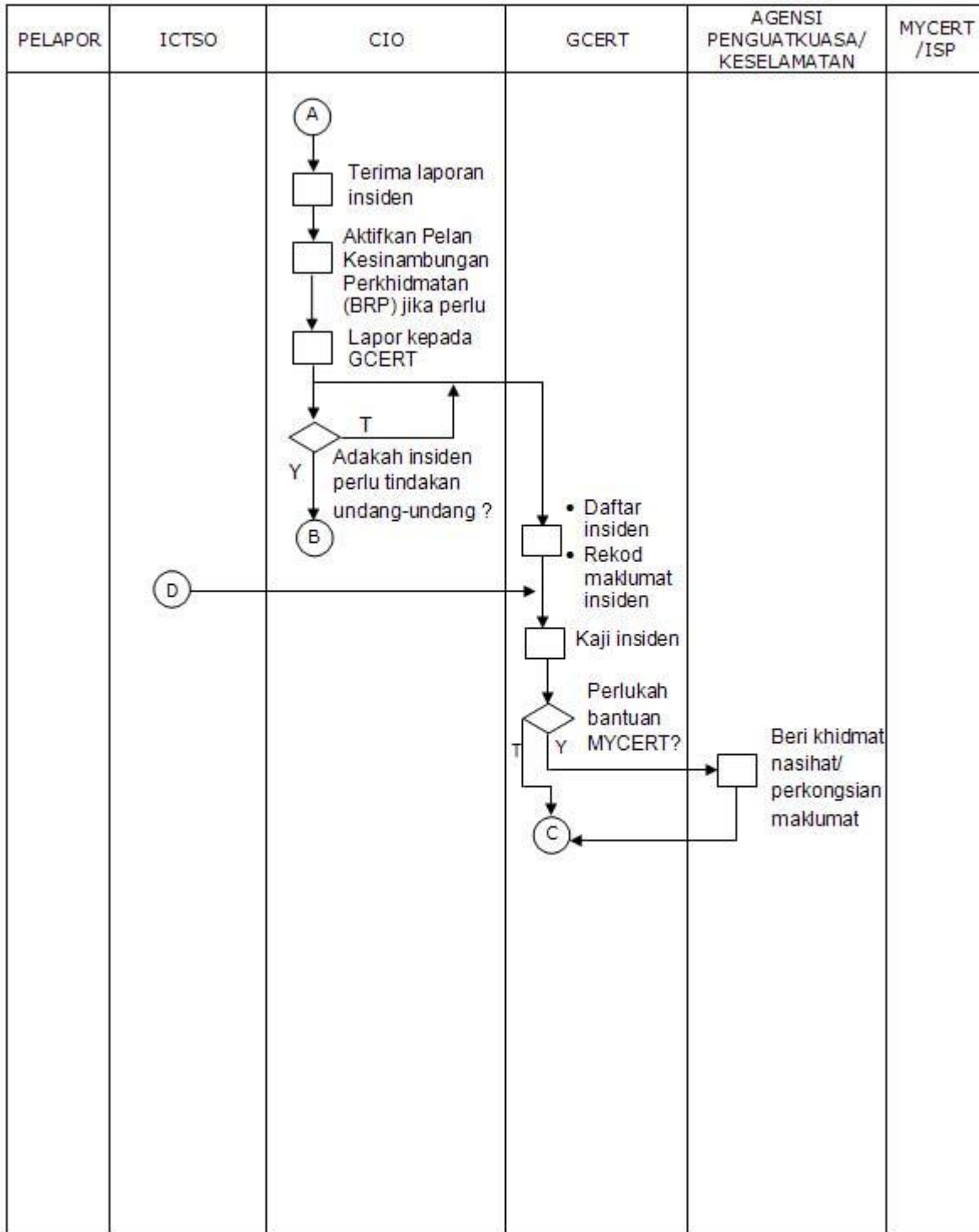
	<ul style="list-style-type: none"><li>g. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam;</li><li>h. Akta Tanda Tangan Digital 1997;</li><li>i. Akta Jenayah Komputer 1997;</li><li>j. Akta Hak cipta (Pindaan) Tahun 1997; dan</li></ul>	
--	--	--

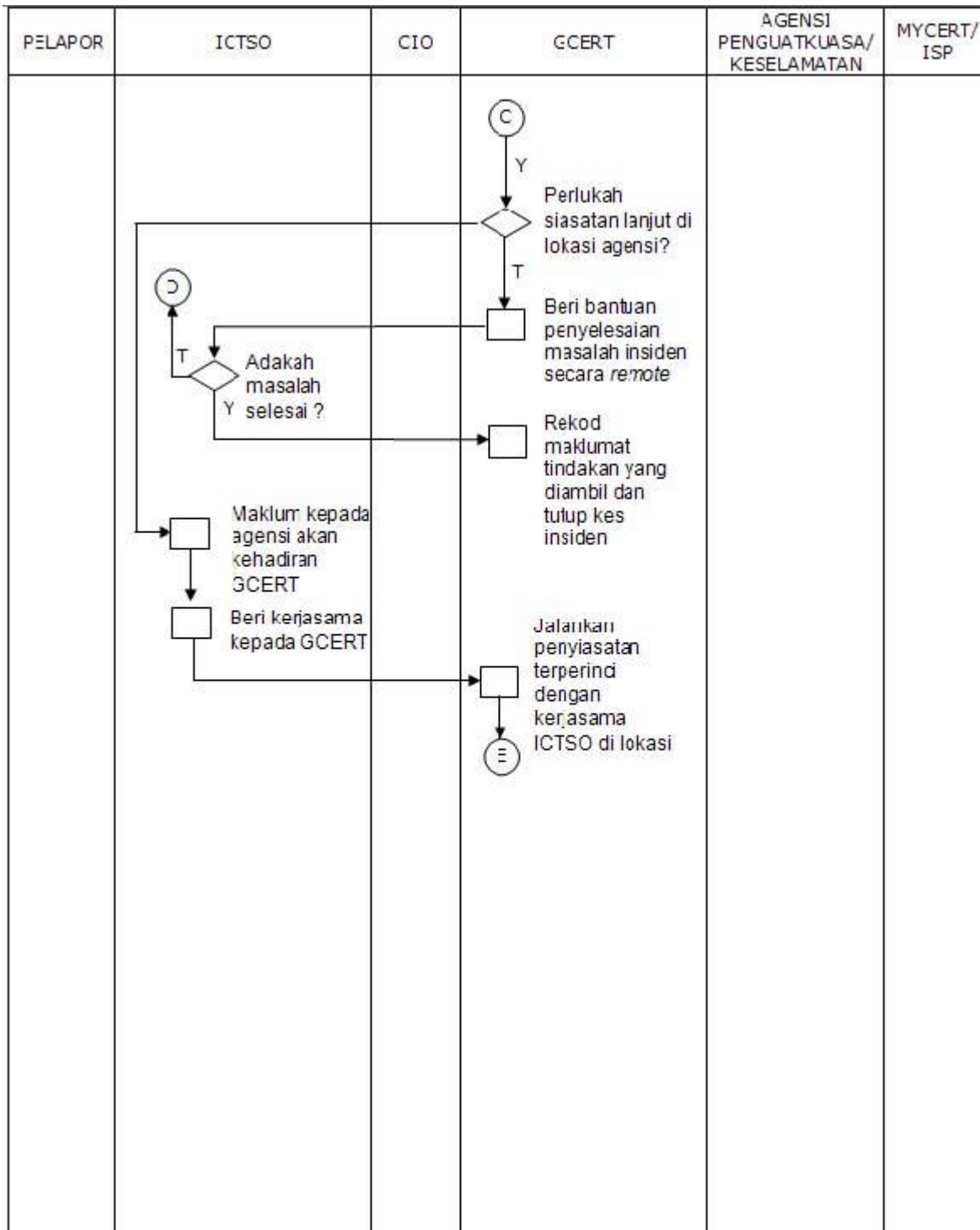
k. Akta Komunikasi dan Multimedia 1998.

LAMPIRAN A

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT KKLW







PELAPOR	ICTSO	CIO	GCERT	AGENSI PENGUATKUASA/ KESELAMATAN	MYCERT/ ISP
			<p>(E)</p> <p>↓</p> <p>□</p> <p>Tindakan IRH di lokasi:-</p> <ul style="list-style-type: none"> <li>• Kawal kerusakan</li> <li>• Baikpulih minima dengan segera</li> <li>• Siasat Insiden dengan terperinci</li> <li>• Analisa Impak (Business Impact Analysis)</li> <li>• Hasilkan laporan Insiden</li> <li>• Bentang dan kemukakan laporan kepada agensi</li> <li>• Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)</li> </ul> <p>↓</p> <p>□</p> <p>Rekod laporan dan tutup kes insiden</p>	<p>(B)</p> <p>↓</p> <p>□</p> <p>Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan</p> <p>(Kerjasama dengan GCERT di lokasi jika perlu)</p>	