



PELABUHAN KUANTAN  
MALAYSIA

# DASAR KESELAMATAN TEKNOLOGI MAKLUMAT

Ver. 2.0



# ISI KANDUNGAN

OBJEKTIF

PENYATAAN KAEDAH

SKOP

PRINSIP-PRINSIP

BIDANG-BIDANG UTAMA

PEMBANGUNAN  
PENYELENGGARA  
AN KAEDAH

KESELAMATAN  
SUMBER MANUSIA

PEROLEHAN,  
PEMBANGUNAN &  
PENYELENGGARAAN  
SISTEM

INFRASTRUKTUR  
ORGANISASI  
DALAMAN

KESELAMATAN  
FIZIKAL DAN  
PERSEKITARAN

PENGURUSAN  
PENGENDALIAN  
INSIDEN  
KESELAMATAN

PENGURUSAN ASET  
ICT

PENGURUSAN  
OPERASI &  
KOMUNIKASI

PENGURUSAN  
KESINAMBUNGAN  
PERKHIDMATAN

KAWALAN CAPAIAN

PEMATUHAN

Glosari

# PENGENALAN

**Kaedah Keselamatan ICT** Lembaga Pelabuhan Kuantan (DKICT LPKtn) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Kaedah ini adalah salah satu kaedah di dalam definisi keselamatan di LPKtn.

Kaedah ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT.

Kaedah ini adalah berdasarkan panduan kepada Dasar Keselamatan ICT yang dikeluarkan oleh pihak MAMPU dan disesuaikan bagi penggunaan LPKtn.

## OBJEKTIF

DKICT LPKtn diwujudkan untuk menjamin kesinambungan urusan LPKtn dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama DKICT LPKtn ialah seperti berikut:

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

# PENYATAAN KAEDAH



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 menyediakan 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:

✓ Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

01

✓ Memastikan setiap maklumat adalah tepat dan sempurna;

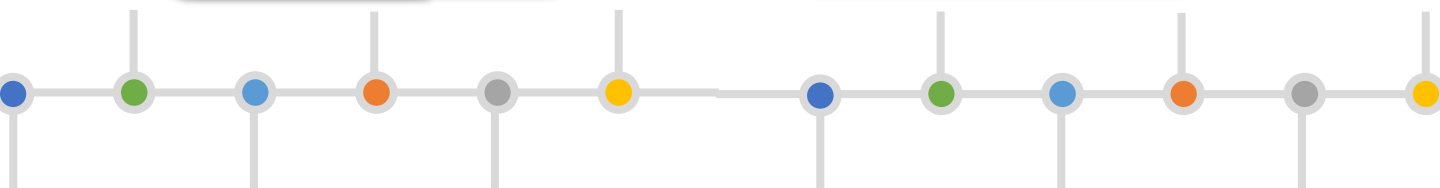
02

✓ Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

03

✓ Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

04



# PENYATAAN KAEDAH

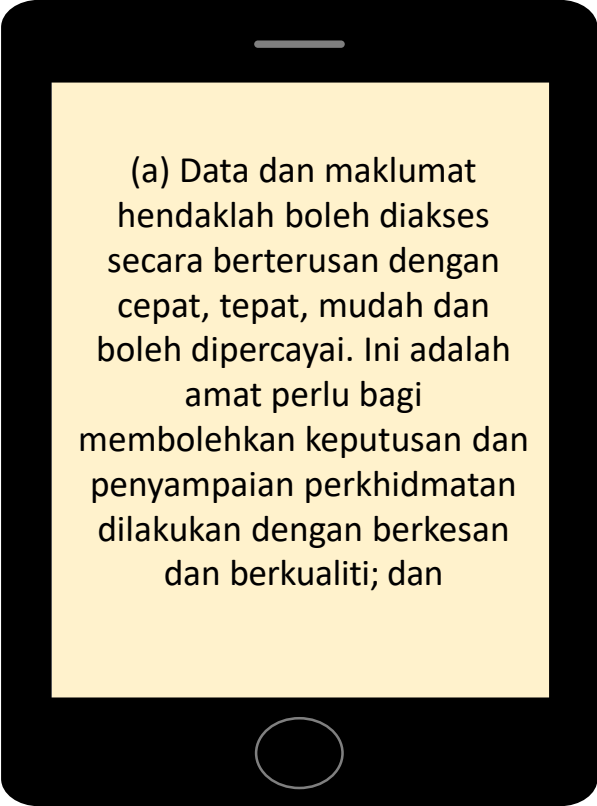
DKICT LPKtn merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:



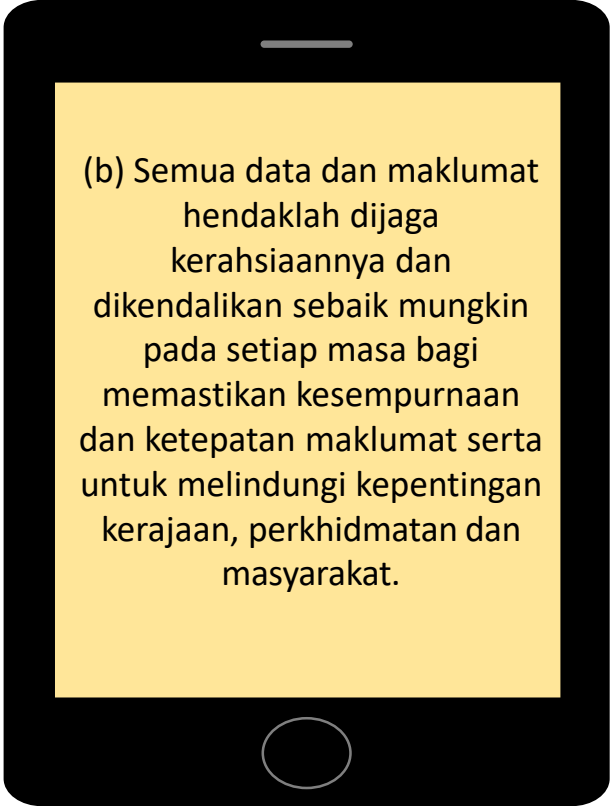
Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan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



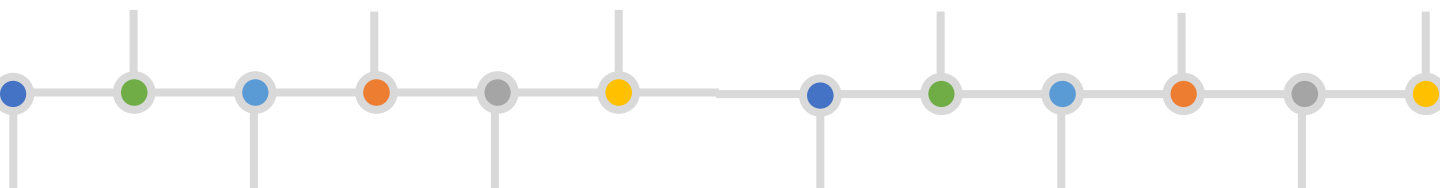
Aset ICT LPKtn terdiri daripada manusia, peralatan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT LPKtn menetapkan keperluan-keperluan asas berikut :



(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, DKICT LPKtn 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:



## Perkakasan

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



## 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 LPKtn;



## Perkhidmatan

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

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



## Data & maklumat

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



## Manusia

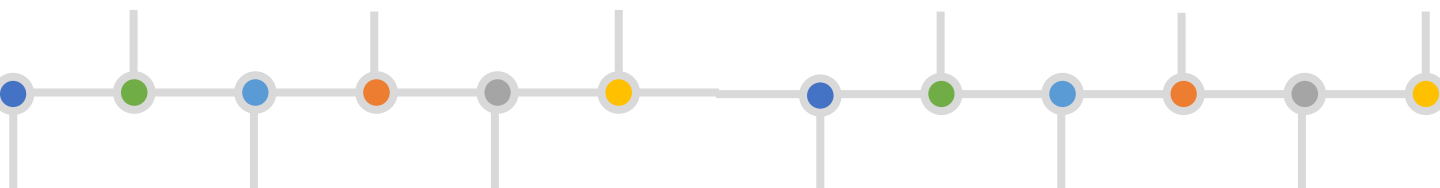
Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian agensi bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.



## Premis, Manusia & 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.





Prinsip-prinsip yang menjadi asas kepada DKICT LPKtn dan perlu dipatuhi adalah seperti berikut:



## 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;

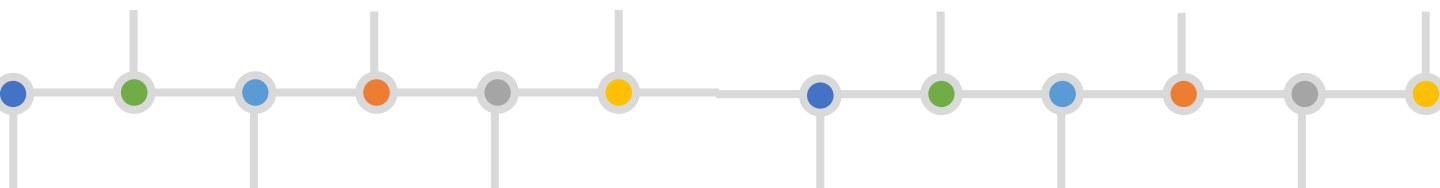
## Perisian

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 LPKtn;



## Hak akses minimum

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

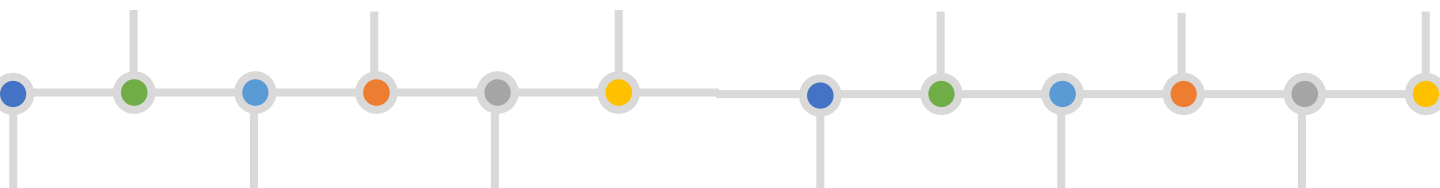




## Akauntabiliti

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 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 standard, 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.





## 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;

## 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;



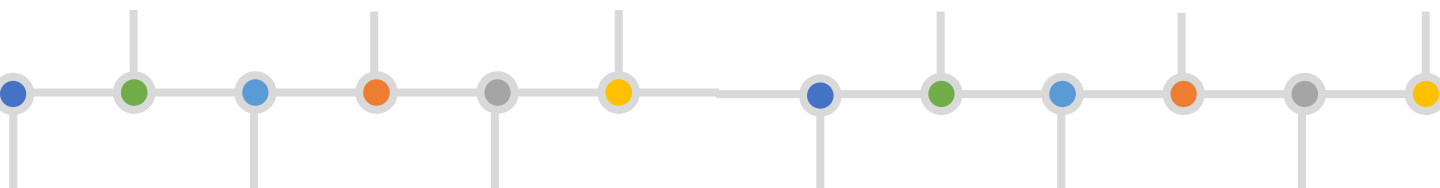
## Pematuhan

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

## 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.





PELABUHAN KUANTAN  
MALAYSIA

A white laptop computer is shown from a front-facing perspective, centered within a large, thin grey circle. The laptop's screen is white and displays the text 'BIDANG-BIDANG UTAMA' in a bold, blue, sans-serif font. The keyboard and trackpad are visible on the laptop's base.

**BIDANG-BIDANG  
UTAMA**

0

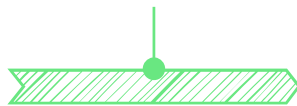
1

# PEMBANGUNAN PENYELENGGARAAN KAEDAH



KAEDAH  
KESELAMATAN ICT

010101



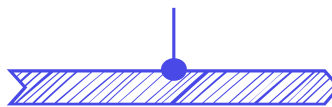
PELAKSANAAN  
KAEDAH

010102



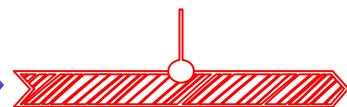
KAEDAH PENYEBARAN

010103

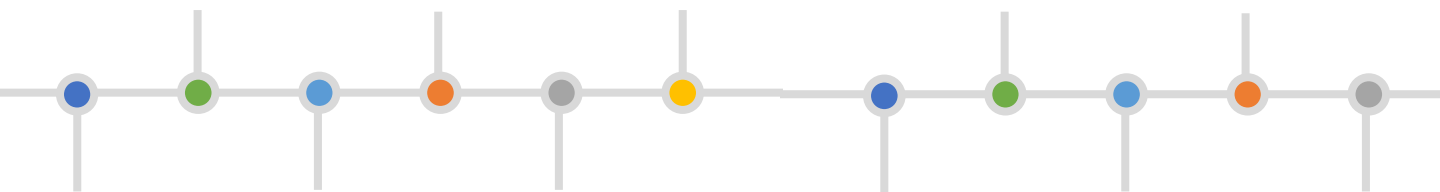


PENYELENGGARAAN

010104



PENGECUALIAN  
KAEDAH





## Kaedah Keselamatan ICT

**Objektif:**

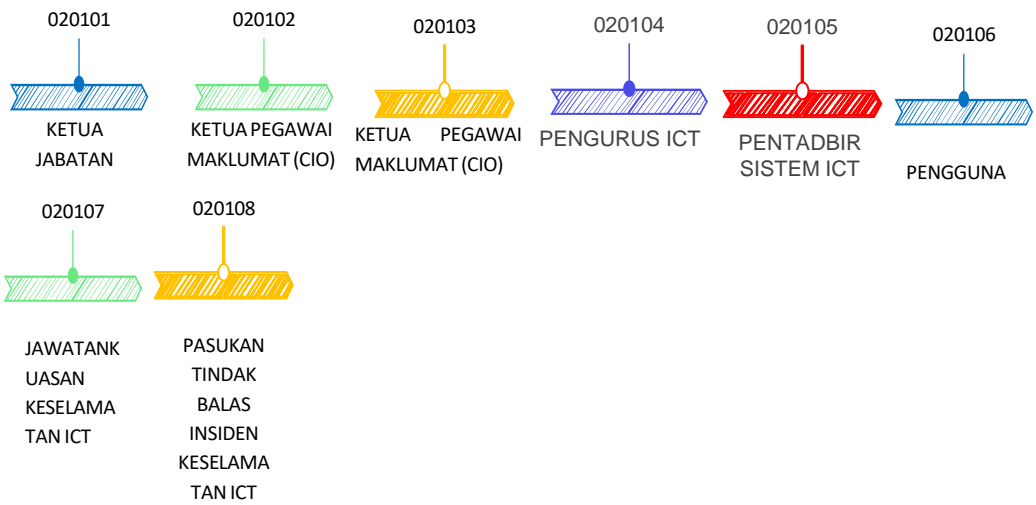
DKICT LPKtn diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran pelaksanaan operasi secara berterusan dan meminimumkan kerosakan atau kemusnahan aset ICT.

Bil	Penerangan	Tindakan
01	<p><b>Pelaksanaan Kaedah</b></p> <p>Ketua Jabatan bertanggungjawab dalam memastikan pelaksanaan DKICT dengan cekap dan berkesan dibantu oleh Jawatankuasa ICT (JKICT) LPKtn atau jawatankuasa yang setara dengannya.</p>	Ketua Jabatan
02	<p><b>Penyebaran Kaedah</b></p> <p>Kaedah ini perlu disebar kepada semua pengguna LPKtn (termasuk kakitangan, pembekal, pakar runding dan lain-lain)</p>	ICTSO
03	<p><b>Penyelenggaraan Kaedah</b></p> <p>DKICT LPKtn adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi Kerajaan dan kepentingan sosial. Berikut adalah prosedur penyelenggaraan DKICT LPKtn:</p> <ul style="list-style-type: none"> <li>✓ Kenal pasti dan tentukan perubahan yang diperlukan;</li> <li>✓ Kemukakan cadangan pindaan secara bertulis kepada CIO LPKtn untuk dibentangkan dalam Mesyuarat JKICT LPKtn atau mesyuarat yang setara dengannya;</li> <li>✓ Perubahan yang telah dipersetujui oleh JKICT LPKtn atau jawatankuasa yang setara dengannya dimaklumkan kepada semua pengguna LPKtn; dan</li> <li>✓ Kaedah ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.</li> </ul>	ICTSO
04	<p><b>Pengecualian Kaedah</b></p> <p>DKICT LPKtn adalah terpakai kepada semua pengguna LPKtn dan tiada pengecualian diberikan.</p>	

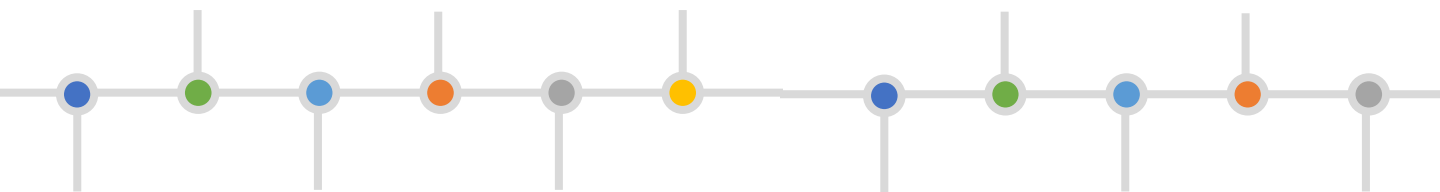
# INFRASTRUKTUR ORGANISASI DALAMAN



INFRASTRUKTUR ORGANISASI DALAMAN



PIHAK KETIGA





## Infrastruktur Organisasi Keselamatan

**Objektif:**

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT LPKtn.

Bil	Penerangan	Tindakan
01	<p><b>Ketua Jabatan</b></p> <p>Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>❖ Memastikan semua pengguna mematuhi peruntukan-peruntukan di bawah DKICT LPKtn;</li> <li>❖ Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan</li> <li>❖ Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT LPKtn.</li> </ul>	Ketua Jabatan
02	<p><b>Ketua Pegawai Maklumat (CIO)</b></p> <p>Jawatan Ketua Pegawai Maklumat (CIO) peringkat LPKtn adalah disandang Pengurus Kanan Korporat dan Pembangunan.</p> <p>Peranan dan tanggungjawab CIO adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>➤ Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;</li> <li>➤ Menentukan keperluan keselamatan ICT;</li> <li>➤ Menyelaraskan dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT LPKtn serta pengurusan risiko dan pengauditan; dan</li> <li>➤ Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT LPKtn.</li> </ul>	ICTSO
03	<p><b>Pegawai Keselamatan ICT (ICTSO)</b></p> <p>Jawatan ICTSO bagi peringkat Lembaga Pelabuhan Kuantan adalah disandang oleh Penolong Pengurus Teknologi Maklumat (PP(IT)).</p> <p>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <ol style="list-style-type: none"> <li>a) Merancang, mengurus dan melaksanakan program keselamatan ICT LPKtn;</li> <li>b) Memberi penerangan dan pendedahan berkenaan DKICT LPKtn kepada semua pengguna;</li> <li>c) Membantu dalam menjalankan pengurusan risiko;</li> <li>d) Mengambil tindakan pembetulan ke atas hasil penemuan audit;</li> <li>e) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian:</li> </ol>	ICTSO

0

2

0

1

## Infrastruktur Organisasi Keselamatan

### Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT LPKtn.

Bil	Perkara
05	<p><b>Pengurus ICT</b></p> <p>Pengurus ICT bagi peringkat LPKtn adalah disandang oleh Ketua Unit IT / Pegawai yang bertanggungjawab ke atas ICT. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</p> <p>(a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan semasa;</p> <p>(b) Menentukan kawalan akses pengguna terhadap aset ICT LPKtn ;</p> <p>(c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO LPKtn;</p> <p>(d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LPKtn.</p>
06	<p><b>Pentadbir Sistem ICT</b></p> <p>Pentadbir Sistem ICT di LPKtn disandang oleh Pengurus IT, Penolong Pegawai Teknologi Maklumat 1 dan Penolong Pegawai Teknologi Maklumat 2.</p> <p>Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>➤ Mengambil tindakan segera apabila kakitangan berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;</li> <li>➤ Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT LPKtn;</li> <li>➤ Memantau aktiviti capaian harian pengguna;</li> <li>➤ Memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;</li> <li>➤ Mengenal pasti aktiviti-aktiviti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan segera;</li> <li>➤ Menyimpan dan menganalisis rekod jejak audit;</li> <li>➤ Menyediakan laporan mengenai aktiviti capaian secara berkala.</li> </ul>

0

2

0

1

## Infrastruktur Organisasi Keselamatan

### Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT LPKtn.

Bil

Perkara

07

### Jawatankuasa Mesyuarat ICT (JPICT) LPKtn

**Jawatankuasa Mesyuarat ICT (JPICT) LPKtn** adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT LPKtn. Keanggotaan Ahli **Jawatankuasa Mesyuarat JPICT LPKtn** adalah seperti berikut:

**Pengerusi:   Pengurus Besar**

**Ahli :           Pengurus Kanan Korporat dan Pembangunan**

**Pengurus Kanan Operasi dan Kawalselia**

**Pengurus Kanan Kewangan Dan Pentadbiran**

**Pengurus IT**

**Penolong Pengurus IT 1**

**Penolong Pengurus IT 2**

**Urus setia:** Unit IT

**Bidang kuasa:**

- ❖ Memperakukan / meluluskan dokumen DKICT LPKtn;
- ❖ Memantau tahap pematuhan keselamatan ICT;
- ❖ Menilai aspek teknikal keselamatan projek-projek ICT;
- ❖ Memperakukan dan meluluskan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT LPKtn;
- ❖ Memastikan sistem ICT sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;
- ❖ Memberi nasihat kepada JPICT dari aspek keselamatan ICT;
- ❖ Menilai kesesuaian teknologi untuk keperluan keselamatan ICT;
- ❖ Memastikan DKICT LPKtn selaras dengan dasar-dasar ICT kerajaan semasa;
- ❖ Membincangkan laporan keselamatan ICT dan menyelesaikan isu-isu berbangkit;
- ❖ Menimbang dan meluluskan Pelan Kesyinambungan Perkhidmatan (BCP) LPKtn.
- ❖ Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan

Membincangkan pelanggaran DKICT LPKtn dan tindakan yang perlu diambil.

0

2

0

1

## Infrastruktur Organisasi Keselamatan

Bil

Perkara

08

**Pasukan Tindak Balas Insiden Keselamatan ICT LPKtn (HelpDesk ICT)**

Keanggotaan CERT LPKtn adalah seperti berikut:

**Keahlian di Peringkat LPKtn****Pengarah :** CIO LPKtn**Pengurus :** ICTSO LPKtn**Urus setia:** Penolong Pegawai Teknologi Maklumat di Unit IT, LPKtn**Keahlian CERT di Peringkat Jabatan****Pengarah :** CIO Jabatan**Pengurus :** ICTSO Jabatan**Ahli :**

Pengurus IT

Penolong Pengurus IT

**Urus setia:** Unit IT

Bagi Jabatan/Agensi yang tidak mempunyai kakitangan Teknologi Maklumat yang mencukupi, CERT Jabatan tidak perlu diwujudkan dan sebarang insiden keselamatan ICT hendaklah dilaporkan terus kepada CERT di peringkat Kementerian.

Peranan dan tanggungjawab Unit IT LPKtn adalah seperti berikut:

- ❖ Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;
- ❖ Merekodkan dan menjalankan siasatan awal insiden yang diterima;
- ❖ Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
- ❖ Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya;
- ❖ Menasihati LPKtn mengambil tindakan pemulihan dan pengukuhan;
- ❖ Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna LPKtn.
- ❖ Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

0

2

0

2

## Pihak Ketiga

### Pihak Ketiga

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

Bil	Perkara
01	<p><b>Keperluan Keselamatan Kontrak dengan Pihak Ketiga</b></p> <p>Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut:</p> <p>(a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemrosesan 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.</p> <p>(d) Perkara-perkara yang perlu dimasukkan dalam perjanjian hendaklah selaras dengan :</p> <ul style="list-style-type: none"> <li>i. DKICT LPKtn;</li> <li>ii. Arahan Keselamatan;</li> <li>iii. Perakuan Akta Rahsia Rasmi 1972; dan</li> <li>iv. Hak Harta Intelek.</li> </ul> <p>Menandatangani “Aku Janji Pematuhan Kaedah Keselamatan LPKtn” bagi mematuhi DKICT LPKtn</p> <p><b>Tindakan oleh:</b> CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga</p>
02	<p><b>Keperluan Mengenalpasti Risiko Keselamatan Maklumat Dalam Pengurusan Projek</b></p> <p>Ini bertujuan memastikan risiko keselamatan maklumat terhadap aktiviti selain daripada rutin seharian iaitu projek dikenalpasti bagi menjamin tiada ketirisan maklumat semasa projek dilaksanakan. Sebarang risiko keselamatan maklumat terhadap projek mestilah direkodkan.</p>

# PENGURUSAN ASET ICT

0301

AKAUNTABILITI  
ASET

INVENTORI ASET  
ICT



030101

0302

PENGELASAN &  
PENGENDALIAN  
MAKLUMAT

PENGELASAN  
MAKLUMAT

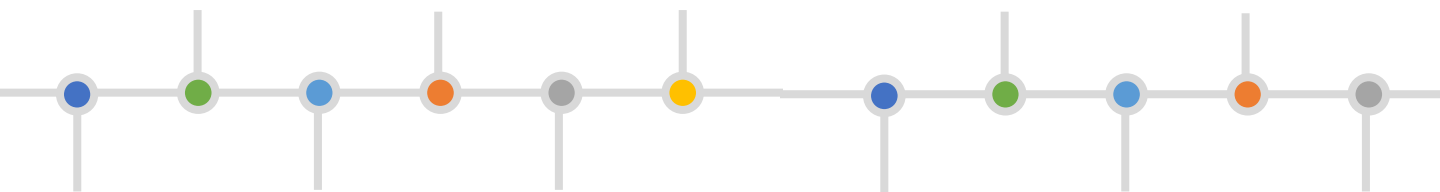


030201

030202



PENGENDALIAN  
MAKLUMAT





### Akauntabiliti Aset

**Objektif:**

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LPKtn.

Bil	Perkara	Tindakan
01	<p><b>Inventori Aset ICT</b></p> <p>Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.</p> <p>Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:</p> <ul style="list-style-type: none"> <li>(a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;</li> <li>(b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;</li> <li>(c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di LPKtn;</li> <li>(d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan</li> <li>(e) Setiap pengguna adalah bertanggungjawab ke atas aset ICT dibawah kawalannya.</li> </ul>	<p>Pentadbir Sistem, Pegawai Aset dan semua pengguna LPKtn</p>



## Pengelasan dan Pengendalian Maklumat

**Objektif:**

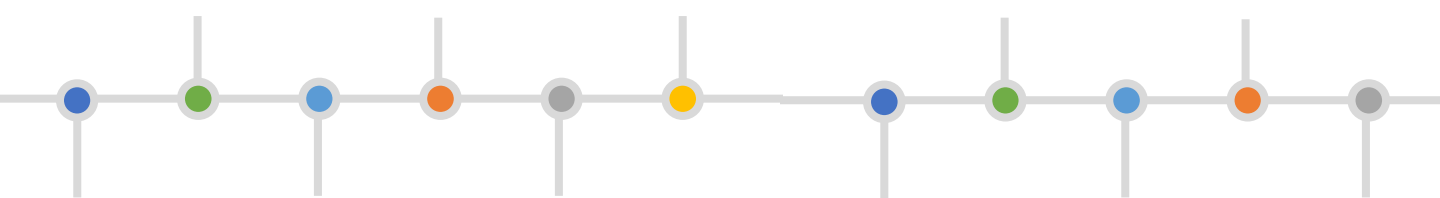
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

Bil	Perkara	Tindakan
01	<p><b>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> <ul style="list-style-type: none"> <li>(a) Rahsia Besar;</li> <li>(b) Rahsia;</li> <li>(c) Sulit; atau</li> <li>(d) Terhad.</li> </ul>	<p>Pegawai Pengelas</p>
02	<p><b>Pengendalian Maklumat</b></p> <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 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 kerahsiaan langkah-langkah keselamatan ICT dari Diketahui umum.</li> </ul>	<p>Semua, Pegawai Pengelas</p>

0 4



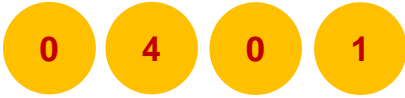
KESELAMATAN  
SUMBER MANUSIA  
DALAM TUGAS  
HARIAN



## 0 4 0 1 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 sertameningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

NO	PENERANGAN	TINDAKAN
01	<p><b>Sebelum Perkhidmatan</b> Perkara-perkara yang mesti dipatuhi termasuk yang berikut:</p> <p>(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.</p> <p>(b) 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.</p> <p>(c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.</p>	Semua



### 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 sertameningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

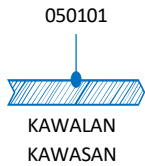
NO	PENERANGAN	TINDAKAN
02	<p><b>Dalam Perkhidmatan</b> Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <p>(a) Memastikan semua pengguna serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan garis panduan dan peraturan serta perundangan berkaitan yang ditetapkan.</p> <p>(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.</p> <p>(c) memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya perlu ke atas semua pengguna, pembekal, pakar runding dan pihak ketiga yang berkepentingan apabila berlaku pelanggaran dengan perundangan dan peraturan ditetapkan.</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>	Semua
03	<p><b>Bertukar Atau Tamat Perkhidmatan</b> 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.</p> <p>(b) membatalkan atau menarik balik semua kebenaran capaian ke atas</p>	

0 5

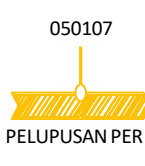
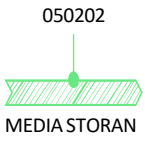
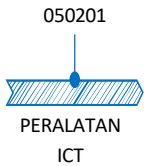
# KESELAMATAN FIZIKAL DAN PERSEKITARAN



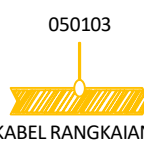
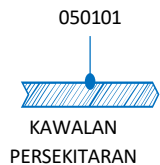
KESELAMATAN KAWASAN



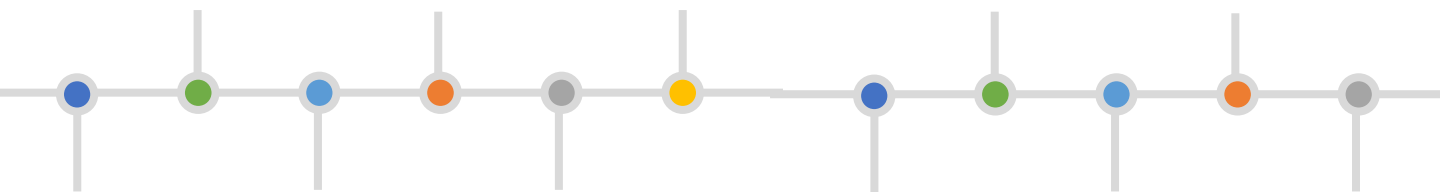
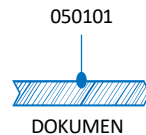
KESELAMATAN PERALATAN



KESELAMATAN PERSEKITARAN



KESELAMATAN DOKUMEN





**Keselamatan Kawasan**

**Objektif :** Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

NO	PENERANGAN	TINDAKAN
01	<p><b>Kawalan Kawasan</b></p> <p>Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <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.</p> <p>(b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemrosesan maklumat.</p> <p>(c) Memastikan alat penggera atau kamera sentiasa berfungsi dengan baik mengikut keperluan.</p> <p>(d) Memastikan kaunter kawalan dan perkhidmatan keselamatan diwujudkan serta menghadkan jalan keluar masuk bagi memastikan pengguna yang dibenarkan sahaja memasuki kawasan tersebut.</p> <p>(e) Menyediakan tempat atau bilik khas untuk pelawat-pelawat.</p> <p>(f) Mereka bentuk dan melaksanakan susun atur keselamatan fizikal di dalam ruang pejabat yang mempunyai kemudahan ICT.</p> <p>(g) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana (force majeure).</p>	<p>Pegawai Keselamatan, CIO dan ICTSO</p>

0

5

0

1

## Keselamatan Kawasan

**Objektif :** Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

NO	PENERANGAN	TINDAKAN
02	<p><b>Kawalan Masuk Fizikal</b></p> <p>Perkara-perkara yang perlu dipatuhi termasuk yang berikut:</p> <p>(a) Semua pengguna hendaklah memakai dan mempamerkan pas keselamatan sepanjang waktu bertugas.</p> <p>(b) Pas keselamatan hendaklah dikembalikan apabila pengguna tidak lagi berkhidmat di LPKtn.</p> <p>(c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter kawalan keselamatan dan hendaklah dikembalikan semula selepas tamat lawatan.</p> <p>(d) Kehilangan pas mestilah dilaporkan dengan kadar segera kepada pihak yang mengeluarkannya.</p>	Semua
03	<p><b>Kawalan Larangan (KTTT)</b></p> <p>Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja mengikut Arahan Keselamatan. Ini dilaksanakan untuk melindungi aset ICT dan berkaitan keselamatan pelabuhan yang terdapat di dalam kawasan tersebut.</p> <p>Perkara-perkara yang perlu dipatuhi di kawasan larangan adalah seperti berikut:</p> <p>(a) Akses kepada kawasan larangan hanyalah kepada pegawai pegawai yang dibenarkan sahaja.</p> <p>(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki</p>	

0

5

0

2

## Keselamatan Peralatan

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
01	<p><b>Peralatan ICT</b></p> <p><b>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</b></p> <p>(a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan.</p> <p>(b) Pengguna bertanggungjawab sepenuhnya ke atas komputer Masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan.</p> <p>(c) Pengguna dilarang sama sekali menambah, menanggalkan atau menukar ganti sebarang perkakasan ICT yang telah ditetapkan tanpa kebenaran.</p> <p>(d) pengguna dilarang membuat sebarang pemasangan (<i>installation</i>) perisian tanpa kebenaran Pentadbir Sistem atau pegawai yang dipertanggungjawabkan.</p> <p>(e) pengguna mestilah memastikan perisian <i>antivirus</i> di komputer mereka dikemas kini dan sentiasa melakukan imbasan ke atas media storan yang digunakan.</p> <p>(f) semua peralatan sokongan ICT hendaklah dilindungi daripada dicuri, dirosakkan, disalah guna dan diubahsuai tanpa kebenaran.</p> <p>(g) setiap pengguna adalah bertanggungjawab ke atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya.</p> <p>(h) peralatan-peralatan kritikal perlu dibekalkan dengan <i>Uninterruptable Power Supply</i> (UPS).</p>	Semua

0

5

0

2

**Keselamatan Peralatan**

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
01	<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 berkuat kuasa.</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 serta maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja.</p> <p>(r) Pengguna hendaklah mematikan suis semua perkakasan ICT apabila meninggalkan pejabat.</p>	Semua

0

5

0

2

## Keselamatan Peralatan

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
02	<p><b>Media Storan</b></p> <p>Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, <i>optical disk</i>, <i>flash disk</i>, CDROM dan media storan lain.</p> <p>Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan.</p> <p>Bagi menjamin keselamatan, perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;</li> <li>(b) bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;</li> <li>(c) semua data di dalam media storan yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;</li> <li>(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;</li> <li>(e) media storan dan peralatan <i>backup</i> hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;</li> <li>(f) media <i>backup</i> hendaklah diletakkan di tempat yang terkawal; dan</li> <li>(g) membuat salinan atau penduaan (<i>data backup</i>) bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.</li> </ul>	Semua

0

5

0

2

**Keselamatan Peralatan**

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
03	<p><b>Media Tandatangan Digital</b></p> <p>Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut:</p> <p>(a) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan.</p> <p>(b) Media ini tidak boleh dipindah-milik atau dipinjamkan,</p> <p>(c) sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.</p>	Semua
04	<p><b>Media Perisian Dan Aplikasi</b></p> <p>Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut:</p> <p>(a) Pegawai hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan</p> <p>(b) Media ini tidak boleh dipindah-milik atau dipinjamkan.</p> <p>(c) sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya</p>	Semua, Pengurus ICT

0

5

0

2

**Keselamatan Peralatan**

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
05	<p><b>Penyelenggaraan Perkakasan</b></p> <p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Bertanggungjawab terhadap penyelenggaraan setiap perkakasan ICT sama ada dalam tempoh jaminan atau telah habis tempoh jaminan</p> <p>(b) semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi yang telah ditetapkan</p> <p>(c) memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja.</p> <p>(d) menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan</p> <p>(e) memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.</p> <p>(f) semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT atau pegawai yang bertanggungjawab</p>	
06	<p><b>Peralatan di Luar Premis</b></p> <p>Perkakasan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Peralatan perlu dilindungi dan dikawal sepanjang masa.</p> <p>(b) Penyimpanan atau penempatan peralatan mestilah mengambil kira</p>	Semua

0

5

0

2

**Keselamatan Peralatan**

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
07	<p><b>Pelupusan Perkakasan</b></p> <p>Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak ekonomik untuk dibaiki sama ada harta modal atau inventori yang dibekalkan.</p> <p>Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat yang terdapat di dalam aset ICT tidak terlepas dari kawalan.</p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat sebelum peralatan ICT dilupuskan</li> <li>(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan</li> <li>(c) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya.</li> <li>(d) peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut.</li> <li>(e) Pegawai aset bertanggungjawab merekodkan butir – butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem yang diguna pakai;</li> </ul>	Semua

0

5

0

2

## Keselamatan Peralatan

**Objektif :** Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian dan gangguan kepada peralatan tersebut.

NO	PENERANGAN	TINDAKAN
07	<p><b>Pelupusan Perkakasan</b></p> <p>(f) pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa.</p> <p>(g) Pengguna ICT adalah <b>DILARANG</b> daripada melakukan perkara-perkara seperti berikut:-</p> <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 LPKtn;</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 LPKtn</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>	Semua

0

5

0

3

**Keselamatan Persekitaran**

**Objektif :** Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

NO	PENERANGAN	TINDAKAN
01	<p><b>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 Pengurus Besar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</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 dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan.</p> <p>(c) peralatan melawan dan mencegah kebakaran (pemadam api, pengesan kebakaran dan sebagainya) hendaklah berfungsi dan diletakkan di tempat yang bersesuaian, mudah dicapai 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)</p>	Semua

0

5

0

3

## Keselamatan Persekitaran

**Objektif :** Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

NO	PENERANGAN	TINDAKAN
02	<p><b>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> <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 <i>Uninterruptable Power Supply</i> (UPS) dan generator tunggu sedia (<i>gen-set</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan.</p> <p>(c) semua peralatan sokongan bekalan kuasa hendaklah di dalam keadaan yang baik, beroperasi penuh dan disemak masa ke semasa.</p>	Bahagian/ Unit IT, ICTSO, Semua

0

5

0

3

## Keselamatan Persekitaran

**Objektif :** Melindungi aset ICT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesusilaan, kecuaiian atau kemalangan.

NO	PENERANGAN	TINDAKAN
03	<p><b>Kabel Rangkaian</b></p> <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>Pihak yang berkaitan / Unit Teknikal / Unit IT, ICTSO,</p>
04	<p><b>Keselamatan Dokumen</b></p> <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 Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan</li> <li>(d) menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.</li> </ul>	<p>Semua</p>

0

5

0

4

**Keselamatan Dokumen**

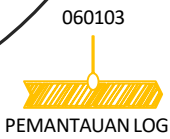
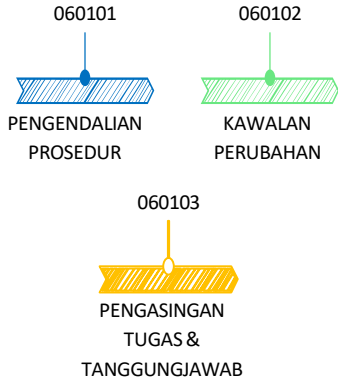
**Objektif :** Melindungi maklumat dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaiian.

NO	PENERANGAN	TINDAKAN
<b>01</b>	<p><b>Dokumen</b></p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan.</p> <p>(b) kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan.</p> <p>(c) pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara.</p> <p>(d) menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.</p>	<p>Pihak yang berkaitan / Unit Teknikal / Unit IT, ICTSO,</p>

# PENGURUSAN OPERASI & KAWALSELIA



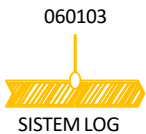
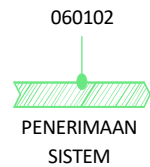
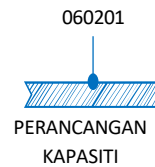
**PENGURUSAN  
PROSEDUR  
OPERASI**



**PENGURUSAN  
PENYAMPAIAN  
PERKHIDMATAN  
PIHAK KETIGA**



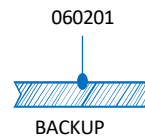
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERISIAN BAHAYA**



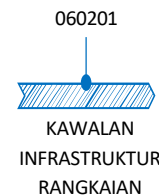
**HOUSEKEEPING**



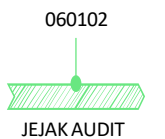
**PENGURUSAN MEDIA**



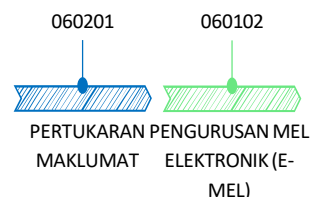
**PENGURUSAN  
RANGKAIAN**



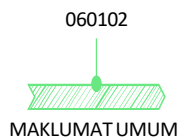
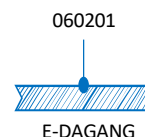
**PENGURUSAN MEDIA**

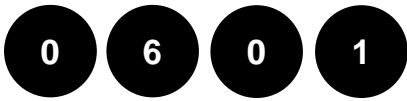


**PENGURUSAN  
PERTUKARAN  
MAKLUMAT**



**PERKHIDMATAN E-  
DAGANG**





**Pengurusan Prosedur Operasi**

**Objektif :** Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

NO	PENERANGAN	TINDAKAN
01	<p><b>Pengendalian Prosedur</b> Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Semua prosedur keselamatan maklumat yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal.</p> <p>(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.</p> <p>(c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.</p>	Semua
02	<p><b>Kawalan Perubahan</b> Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu.</p> <p>(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.</p> <p>(c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah 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 sengaja.</p>	Semua



**Pengurusan Prosedur Operasi**

**Objektif :** Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

NO	PENERANGAN	TINDAKAN
03	<p><b>PENGASINGAN TUGAS DAN TANGGUNGJAWAB</b></p> <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 terperinci atau di manipulasi.</p> <p>(c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian jika perlu.</p>	Semua

0 6 0 2 **Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**

**Objektif :** Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

NO	PENERANGAN	TINDAKAN
01	<p><b>Perkhidmatan Penyampaian</b></p> <p>Perkara-perkara yang mesti dipatuhi termasuk yang berikut:</p> <p>(a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga;</p> <p>(b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa.</p> <p>(c) Pengurusan ke atas perubahan kaedah perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian risiko.</p>	<p>Pengurus ICT, ICTSO</p>



**Perancangan dan Penerimaan Sistem**

**Objektif :** Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

NO	PENERANGAN	TINDAKAN
01	<p><b>Perancangan Kapasiti</b></p> <p>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> <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>	Pengurus ICT, ICTSO
02	<p><b>Penerimaan Sistem</b></p> <p>Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.</p>	Pengurus ICT, ICTSO



**Perisian Berbahaya**

**Objektif :** Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

NO	PENERANGAN	TINDAKAN
01	<p><b>Perlindungan dari Perisian Berbahaya</b></p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>a) Memasang sistem keselamatan untuk mengesan perisian ataupun program berbahaya seperti anti virus, <i>Intrusion Detection System (IDS)</i> dan <i>Intrusion Prevention System (IPS)</i> serta mengikut prosedur penggunaan yang betul dan selamat.</li> <li>b) Memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa.</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</li> </ul>	<p>Pengurus ICT, ICTSO</p>

0 6 0 5 HOUSEKEEPING

Objektif : Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

NO	PENERANGAN	TINDAKAN
01	<p><b>Backup</b></p> <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) LPKtn hendaklah menyimpan <i>backup</i> mengikut keperluan atau sekurang-kurangnya satu (1) generasi <i>backup</i>.</p> <p>(e) Merekodkan dan menyimpan salinan <i>backup</i> di lokasi yang berlainan dan selamat</p> <p>(f)Tempoh penyimpanan <b>Salinan backup hendaklah sekurang-kurangnya disimpan selama 5 tahun. Sekiranya lebih daripada tempoh tersebut, data backup boleh dilupuskan sekiranya memerlukan.</b></p>	Semua



PENGURUSAN RANGKAIAN

Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

NO	PENERANGAN	TINDAKAN
01	<p><b>Kawalan Infrastruktur Rangkaian</b></p> <p>Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.</p> <p>Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>a) Semua 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) <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 LPKtn;</li> <li>f) Semua perisian <i>sniffer</i> atau <i>network analyser, proxy</i> dan sebarang perisian penggodam adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.</li> <li>g) Memasang perisian <i>Intrusion Prevention System (IPS)</i> bagi mengesan sebarang cubaan mencerooboh dan aktiviti-</li> </ul>	Unit IT / Pegawai bertanggung jawab

0 6 0 7

**Pengurusan Media**

Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

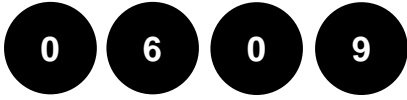
NO	PENERANGAN	TINDAKAN
01	<p><b>Penghantaran dan Pemindahan</b></p> <p>Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.</p>	Semua
02	<p><b>Prosedur Pengendalian Media</b></p> <p>Di antara prosedur-prosedur pengendalian media termasuk:</p> <ul style="list-style-type: none"> <li>a) Melabelkan semua media mengikut tahap keselamatan sesuatu maklumat.</li> <li>b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja.</li> <li>c) Menghadkan 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> <li>e) Menyimpan semua media di tempat yang selamat.</li> <li>f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat</li> </ul>	Semua



**Pengurusan Pertukaran Maklumat**

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

NO	PENERANGAN	TINDAKAN
01	<p>Pertukaran Maklumat</p> <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 LPKtn dengan pihak luar;</p> <p>(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari LPKtn.</p>	Semua
02	<p><b>Pengurusan Mel Elektronik (E-mel)</b></p> <p>Penggunaan e-mel di LPKtn hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan tatacara penggunaan e-mel dan Internet yang terkandung dalam Tatacara Penggunaan E-Mel Dan Internet LPKtn.</p>	Semua



**Perkhidmatan e-DAGANG (Electronic Commerce Services)**

**Objektif :** Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

NO	PENERANGAN	TINDAKAN
01	<p><b>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.</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>	Semua
02	<p><b>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</li> </ul>	Semua

0 6 1 0 Pemantauan

Objektif : Memastikan pengesanan aktiviti pemprosesan yang tidak dibenarkan

NO	PENERANGAN	TINDAKAN
01	<p><b>Pengauditan dan Forensic ICT</b></p> <p>ICTSO mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut:</p> <p>(a) Sebarang percubaan pencerobohan kepada sistem ICT LPKtn</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 membebankan <i>bandwidth</i> rangkaian.</p> <p>(g) aktiviti penyalahgunaan akaun e-mel,</p> <p>(h) aktiviti penukaran <i>IP address</i> selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem.</p>	Semua
02	<p><b>Jejak Audit</b></p> <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>	Semua

0 6 1 0 **Pemantauan**

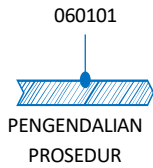
**Objektif : Memastikan pengesanan aktiviti pemprosesan yang tidak dibenarkan**

<b>03</b>	<p><b>Sistem Log</b></p> <p>Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut:</p> <p>(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;</p> <p>(b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera.</p> <p>(c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO, Pengurus ICT dan CIO.</p>	Semua
<b>04</b>	<p><b>Pemantauan Log</b></p> <p>lanya bertujuan untuk memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut:</p> <p>(a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;</p> <p>(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala;</p> <p>(c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;</p> <p>(d) Aktiviti pentadbiran dan operator/pengendali sistem perlu direkodkan;</p> <p>(e) Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan</p> <p>(f) Penyelarasan masa bagi domain keselamatan perlu menggunakan sumber masa yang sama (time synchronization). LPKtn menggunakan sumber melalui SIRIM Malaysia (mst.sirim.my) sebagai rujukan utama.</p>	Semua

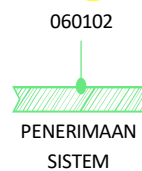
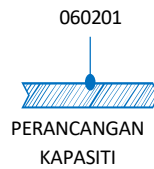
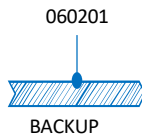
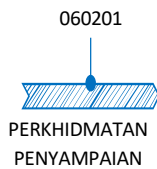
# KAWALAN CAPAIAN



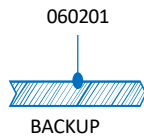
PENGURUSAN  
PROSEDUR  
OPERASI



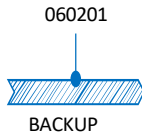
PENGURUSAN  
PENYAMPAIAN  
PERKHIDMATAN  
PIHAK KETIGA



PERANCANGAN &  
PENERIMAAN  
SISTEM



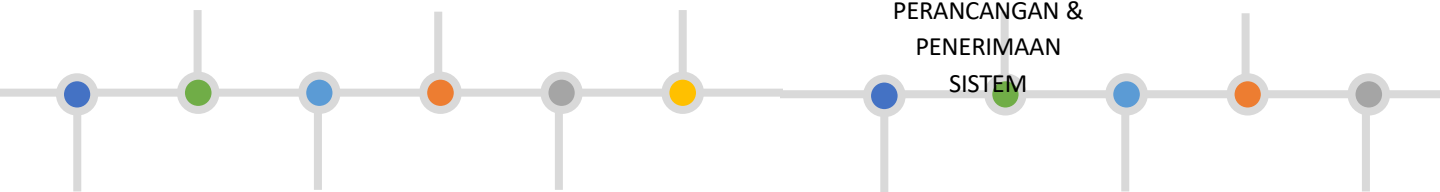
PERANCANGAN &  
PENERIMAAN  
SISTEM



PERANCANGAN &  
PENERIMAAN  
SISTEM



PERANCANGAN &  
PENERIMAAN  
SISTEM





## Kaedah Kawalan Capaian

Objektif : Mengawal capaian ke atas maklumat.

# 01

### Keperluan Kawalan Capaian

Semua

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong kaedah kawalan capaian pengguna sedia ada.

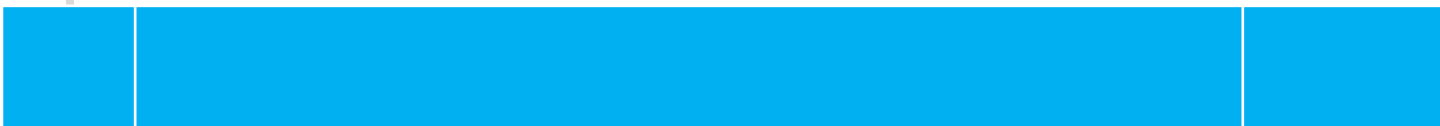
Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna.
- (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran.
- (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih.
- (d) Kawalan ke atas kemudahan pemrosesan maklumat.



**Pengurusan Capaian Pengguna**

**Objektif : Mengawal capaian pengguna ke atas aset ICT.**



**01**

**Akaun Pengguna**

Semua

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:

- (a) akaun yang diperuntukkan oleh LPKtn sahaja boleh digunakan;
- (b) akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
- (c) akaun pengguna yang diwujudkan pertama kali akan diberi hak capaian (access right) paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan hak capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- (d) pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LPKtn. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- (e) penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
- (f) Pentadbir Sistem ICT boleh membekukan dan menamatkan akaun pengguna atas sebab-sebab berikut;
  - i. Pengguna dari Kumpulan Sokongan yang bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi sebulan;
  - ii. Bertukar bidang tugas kerja;
  - iii. Bertukar ke agensi lain;
  - iv. Bersara; atau
  - v. Ditamatkan perkhidmatan.

**02**

**Hak Capaian**

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

Hak capaian sistem pengguna perlu disemak setiap 6 bulan.

0

7

0

2

## Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT.

**03**

### Pengurusan Kata Laluan

Semua

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 LPKtn seperti berikut:

- (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun
- (b) pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi
- (c) panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (Alphanumeric)
- (d) kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun
- (e) kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama
- (f) kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program.
- (g) kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula
- (h) kata laluan hendaklah berlainan daripada pengenalan identiti pengguna
- (i) tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan

0

7

0

2

## Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT.

**04**

### Clean Desk & Clear Screen

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk & Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer.
- (b) menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci
- (c) memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.
- (d) Nilai minimum bagi *lock apps/device* : 10 minit. Bergantung kepada sistem-sistem dan kekangan serta permintaan pengguna.

0

7

0

3

## Kawalan Capaian Rangkaian

**Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.**

<h1>01</h1>	<p><b>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 LPKtn, rangkaian agensi lain dan rangkaian awam.</p> <p>(b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya.</p> <p>(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.</p>	<p>Pentadbir Sistem ICT dan ICTSO</p>
<h1>02</h1>	<p><b>Capaian Internet</b></p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(a) Penggunaan Internet di LPKtn 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 LPKtn</p> <p>(b) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya</p> <p>(c) Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan</p> <p>(d) Penggunaan teknologi <i>packet shaper</i> untuk mengawal aktiviti (videoconferencing, <i>video streaming</i>, <i>chat</i>, <i>downloading</i>) adalah perlu bagi menguruskan penggunaan <i>bandwidth</i> yang maksimum dan</p>	

0

7

0

3

## Kawalan Capaian Rangkaian

**Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.**

**02**

(f) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan

(g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara

(h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LPKtn

(i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada Kaedah dan peraturan yang telah ditetapkan

(j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali kecuali dengan kebenaran khas

(k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

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

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan

0

7

0

3

## Kawalan Capaian Rangkaian

Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

03

### Capaian Jarak Jauh

Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

- (a) Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah Remote Access mestilah menggunakan kaedah penyulitan (encryption).
- (b) Lokasi bagi akses ke sistem ICT LPKtn hendaklah dipastikan selamat.
- (c) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada CIO/Pengurus ICT/kakitangan unit IT, LPKtn. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.
- (d) Penggunaan perisian capaian Jarak Jauh adalah ditentukan, dibenarkan, dipasangkan, diluluskan dan dikonfigurasi oleh HANYA kakitangan Unit IT, LPKtn.

0

7

0

4

## Kawalan Capaian System Pengoperasian

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

01

### Capaian Sistem Pengoperasian

Semua

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:

- (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan
- (b) merekodkan capaian yang berjaya dan gagal.

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

- (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan;
- (b) mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan
- (c) menjana amaran (alert) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

- (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin;
- (b) mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
- (c) menghadkan dan mengawal penggunaan program; dan
- (d) menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi

0

7

0

4

## Kawalan Capaian System Pengoperasian

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

02

### Kad Pintar

Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Penggunaan kad pintar kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yang dikhususkan.
- (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain.
- (c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga(3) kali cubaan akan disekat.
- (d) Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pegawai yang dipertanggungjawabkan.

0

7

0

5

## Kawalan Capaian Aplikasi dan Maklumat

**Objektif:** Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi

**01**

### Capaian Aplikasi dan Maklumat

Semua

Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di LPKtn adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:

- (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut hak capaian dan keselamatan maklumat yang telah ditentukan;
- (b) setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
- (c) menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
- (d) memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;
- (e) capaian sistem maklumat dan aplikasi melalui jarak jauh adalah

0

7

0

6

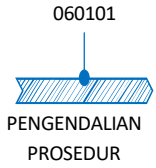
## Peralatan Mudah Alih dan Kerja Jarak Jauh

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

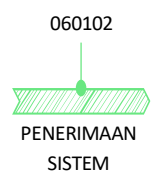
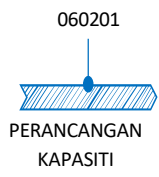
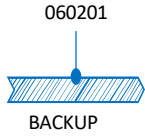
<b>01</b>	<b>Peralatan Mudah Alih</b> Perkara yang perlu dipatuhi adalah seperti berikut:  (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	<b>Semua</b>
<b>02</b>	<b>Kerja Jarak Jauh</b> Perkara yang perlu dipatuhi adalah seperti berikut:  (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	



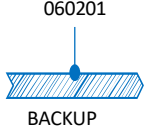
**PENGURUSAN  
PROSEDUR  
OPERASI**



**PENGURUSAN  
PENYAMPAIAN  
PERKHIDMATAN  
PIHAK KETIGA**



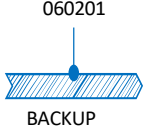
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



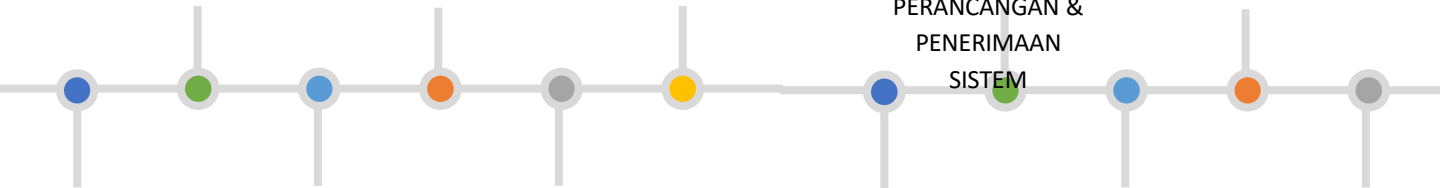
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**





## Keselamatan Dalam Membangunkan Sistem dan Aplikasi

**Objektif :** Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

<p><b>01</b></p>	<p><b>Keperluan Keselamatan Sistem Aplikasi</b></p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut :</p> <p>(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;</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) 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>	<p>Pemilik Sistem, Pentadbir Sistem ICT, ICTSO</p>
<p><b>02</b></p>	<p><b>Pengesahan Data Input</b></p> <p>Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.</p>	<p>Pemilik Sistem dan Pentadbir Sistem ICT</p>
<p><b>03</b></p>	<p><b>Pengesahan Data Output</b></p> <p>Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.</p>	<p>Pemilik Sistem dan Pentadbir Sistem ICT</p>

0

8

0

2

## Kawalan Kriptografi

**Objektif:** Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

<b>01</b>	<b>Penyulitan</b>  Penggunaan tandatangan digita adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi rahsia rasmi secara elektronik.	<b>Semua</b>
<b>02</b>	<b>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.	<b>Semua</b>

0

8

0

3

## Keselamatan Fail System

**Objektif:** Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

# 01

### Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

**Pemilik Sistem dan Pentadbir Sistem ICT**



## Keselamatan Dalam Proses Pembangunan dan Sokongan

**Objektif:** Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

<p><b>01</b></p>	<p><b>Prosedur Kawalan Preubahan</b></p> <p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none"> <li>(a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai</li> <li>(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.</li> <li>(c) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor</li> <li>(d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja</li> <li>(e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan</li> <li>(f) Menghalang sebarang peluang untuk membocorkan maklumat.</li> </ul>	<p>Pemilik Sistem dan Pentadbir Sistem ICT / Urusetia ISMS</p>
<p><b>02</b></p>	<p><b>Pembangunan Secara Outsource</b></p> <p>Pembangunan perisian aplikasi secara outsource perlu dipantau oleh pemilik sistem.</p>	<p>Pentadbir Sistem ICT</p>

0

8

0

5

## Kawalan Teknikal Keterdedahan (Vulnerability)

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

01

### Kawalan dari Ancaman Teknikal

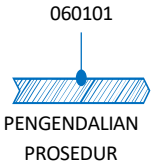
Pentadbir Sistem ICT

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

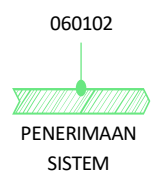
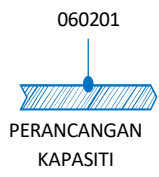
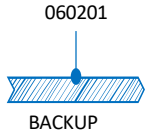
- (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan
- (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi
- (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.



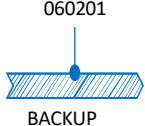
**PENGURUSAN  
PROSEDUR  
OPERASI**



**PENGURUSAN  
PENYAMPAIAN  
PERKHIDMATAN  
PIHAK KETIGA**



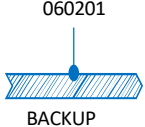
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



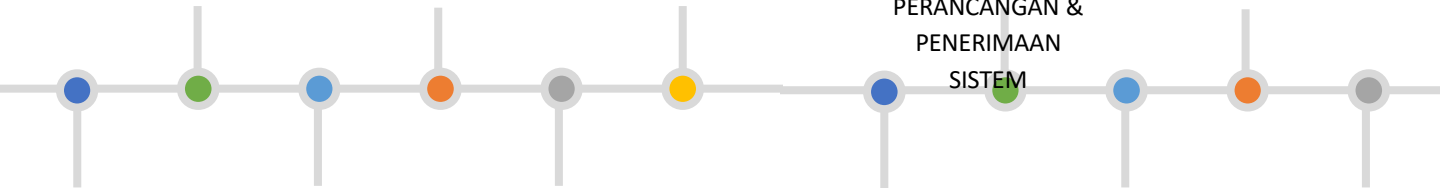
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



0

9

0

1

## Mekanisme Pelaporan Insiden Keselamatan ICT

**Objektif:** Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

01

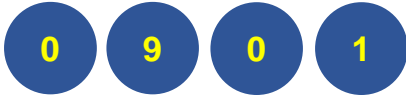
### (a) Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar kaedah keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:

- (a) Maklumat didapati hilang, didedahkan kepada pihak –pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- (c) Kata laluan atau mekanisma kawalan akses:
  - i. hilang, dicuri atau didedahkan;
  - ii. disyaki hilang, dicuri atau didedahkan;
- (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
- (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

- (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
- (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.



## Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

### (b) Mekanisme Pelaporan Selain ICT

Kaedah ini bertujuan bagi memastikan semua insiden dan potensi insiden keselamatan maklumat di LPKtn dilaporkan dan diambil tindakan dengan berkesan. Ini merangkumi semua insiden fizikal yang berlaku ke atas aset maklumat di LPKtn seperti berikut :

- Pelanggaran Dasar (*Violation of Policy*)
- Penghalang Penyampaian Perkhidmatan
- Pencerobohan (*Intrusion*)
- Pemalsuan (*Forgery*)
- Gangguan / Ancaman (*Harrasment / Threats*)
- Percubaan / Mengumpul Maklumat (*Attempts / Hack Threats / Information Gathering*)
- Kehilangan Fizikal (*Physical Loss*)

Pindaan maklumat secara tidak sah

0

9

0

2

## Pengurusan Maklumat Insiden Keselamatan ICT

**Objektif:** Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

**01**

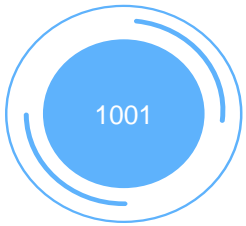
### Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang.

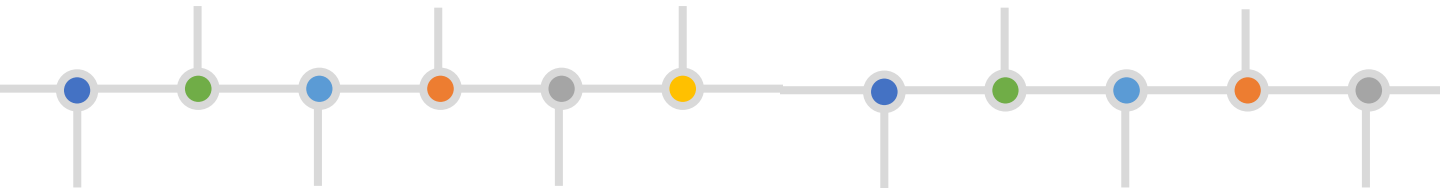
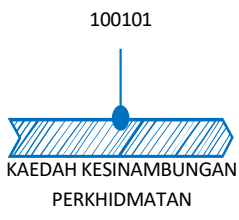
Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada LPKtn.

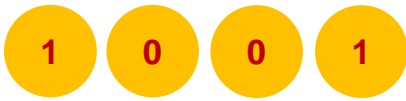
Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut;

- (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;
- (b) menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- (c) menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- (d) menyediakan tindakan pemulihan segera; dan
- (e) memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.



**PENGURUSAN PROSEDUR  
OPERASI**





## KAEDAH KESINAMBUNGAN PERKHIDMATAN

**Objektif:** Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

01

### Pelan Kesinambungan Perkhidmatan

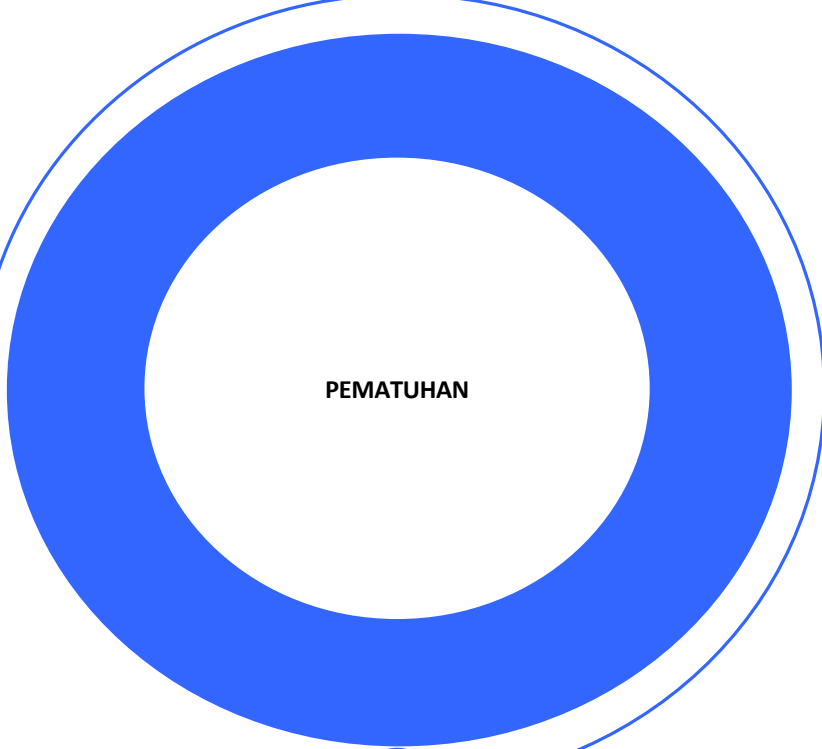
Pengurus ICT

Pelan Kesinambungan Perkhidmatan (Business Continuity Management - 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 Mesyuarat JKICT LPKtn dan perkara-perkara berikut perlu diberi perhatian:

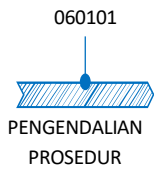
- (a) mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
- (b) melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
- (c) mendokumentasikan proses dan prosedur yang telah dipersetujui;
- (d) mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
- (e) membuat backup;
- (f) menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau mengikut keperluan; dan
- (g) mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap sistem penyampaian perkhidmatan, bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

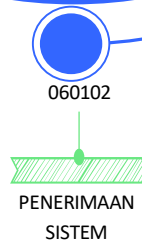
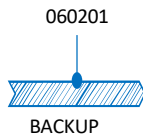
- (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
- (b) Senarai personal LPKtn dan vendor berserta nombor yang boleh



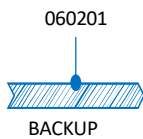
**PENGURUSAN  
PROSEDUR  
OPERASI**



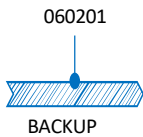
**PENGURUSAN  
PENYAMPAIAN  
PERKHIDMATAN  
PIHAK KETIGA**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



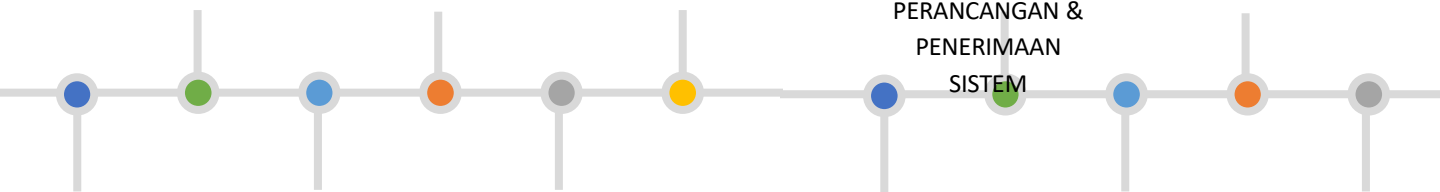
**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



**PERANCANGAN &  
PENERIMAAN  
SISTEM**



1

1

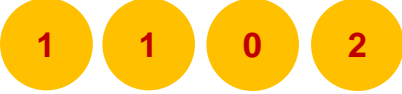
0

1

## Pematuhan dan Keperluan Perundangan

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	<p><b>Pematuhan Kaedah</b></p> <p>Setiap pengguna LPKtn hendaklah membaca, memahami dan mematuhi DKICT LPKtn dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.</p> <p>Semua aset ICT LPKtn termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan.</p> <p>Pegawai yang diturunkan kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.</p> <p>Sebarang penggunaan aset ICT LPKtn selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber LPKtn.</p>	<p>Semua</p> <p>Ketua Jabatan atau pegawai yang diturunkan kuasa</p>



### Pematuhan dan Keperluan Perundangan

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	<p><b>Pematuhan dengan Kaedah, Piawaian dan Keperluan</b></p> <p>Memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi kaedah, piawaian dan keperluan teknikal. Sistem ICT perlu diperiksa secara berkala bagi memastikan standard pelaksanaan keselamatan ICT sentiasa dipatuhi.</p>	ICTSO

1

1

0

3

## Pematuhan Keperluan Audit

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	<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>	Semua

1

1

0

4

## Keperluan Perundangan

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	<p>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di LPKtn:</p> <p>(a) Arahan Keselamatan.</p> <p>(b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan".</p> <p>(c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002.</p> <p>(d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT).</p> <p>e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan".</p> <p>(f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.</p> <p>(g) Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam".</p>	Semua

1

1

0

4

## Keperluan Perundangan

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	<p>(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.</p> <p>(i) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh pada 1 Jun 2007.</p> <p>(j) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.</p> <p>k) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa/Jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan(JITIK).</p> <p>(l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)-“Tatacara Penyediaan, Penilaian dan Penerimaan Tender”.</p> <p>(m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - “Peraturan Perolehan Perkhidmatan Perundangan”;</p> <p>(o) Akta Rahsia Rasmi 1972;</p> <p>(p) Akta Jenayah Komputer 1997;</p>	Semua

1

1

0

4

## Keperluan Perundangan

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	((q) Akta Hak cipta (Pindaan) Tahun 1997. (r) Akta Komunikasi dan Multimedia 1998. (s) Perintah-Perintah Am. (t) Arahan Perbendaharaan. (u) Arahan Teknologi Maklumat 2007. (v) Tatacara Penggunaan E-mail dan Internet. (w) Standard Operating Procedure (SOP) ICT LPKtn. (x) Polisi, standard, SOP LPKtn/Jabatan yang berkaitan. Akta Perlindungan Data Peribadi 2010	Semua



### Pelanggaran Kaedah

**Objektif:** Meningkatkan tahap keselamatan ICT bagi mengelakkan sebarang pelanggaran kepada DKICT LPKtn.

NO	PENERANGAN	TINDAKAN
01	Pelanggaran DKICT LPKtn boleh dikenakan tindakan tatatertib.	Semua

1

1

0

5

**Keselamatan Maklumat bagi Penggunaan  
Perkhidmatan Pengkomputeran Awan ##(5.23)**

NO	PENERANGAN	TINDAKAN
01	<p>Pelan Perolehan (Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam (Kuat kuasa mulai 15 April 2022)).</p> <p>ii) Dasar Perkhidmatan Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam</p> <p>iii) Dengan peningkatan insiden penggodaman berprofil tinggi dan kewajipan undang-undang dan kawal selia yang lebih ketat, adalah penting untuk memastikan maklumat disimpan dan dipantau dengan betul dalam storan 'cloud'</p> <p>Contoh kawalan untuk penggunaan perkhidmatan storan 'cloud' :</p> <ul style="list-style-type: none"> <li>• Proses penglibatan dan penilaian pembekal yang mantap Memastikan pengguna memahami dan sentiasa menyemak Model Tanggungjawab Bersama dan perjanjian kontrak anda (termasuk Perjanjian Tahap Perkhidmatan (SLA))</li> <li>• Kesedaran keselamatan yang kukuh, terutamanya mengenai topik seperti 'malware, phishing' dan sebagainya.</li> <li>• Meningkatkan keselamatan dengan solusi seperti firewalls, anti-virus, encryption methods, internet security tools, mobile device security, intrusion detection tools agar lebih sukar untuk digodam atau membenarkan akses pihak ketiga.</li> <li>• Melaksanakan dasar kata laluan yang kukuh. ggaran DKICT LPKtn boleh dikenakan tindakan tatatertib.</li> </ul>	Semua

1

1

0

5

**Kesediaan ICT untuk kelangsungan Perniagaan  
##(5.30)**

NO	PENERANGAN	TINDAKAN
01	<p>Kesediaan ICT hendaklah dirancang, diselenggara dan diuji kesediaannya berdasarkan keperluan perniagaan. Kesediaan ICT wujud daripada gambaran yang lebih besar tentang kesediaan perniagaan ( objektif semasa pemulihan ICT)</p> <p>Contoh kawalan pelaksanaan kesediaan ICT:</p> <ul style="list-style-type: none"> <li>• Masa pemulihan ICT diperoleh daripada penilaian impak perniagaan organisasi.</li> <li>• Pelan diwujudkan berdasarkan strategi sekiranya ICT tidak tersedia (DRC, pemulihan in-situ, insurans, peralatan ganti, sandaran, ketersediaan tinggi)</li> <li>• Pelan ujian ICT BCP diuji berdasarkan senario risiko yang berbeza untuk mengukur masa pemulihan.</li> <li>• Jika infrastruktur berada dalam storan cloud, pantau secara berterusan dengan jelas jaminan ketersediaan daripada pembekal servis storan 'cloud' dan pastikan tanggungjawab untuk kesinambungan diterangkan dalam hubungan.</li> </ul>	Semua

1

1

0

5

'Data Deletion' ##8.10

NO	PENERANGAN	TINDAKAN
01	<p>Maklumat harus dipadamkan apabila tidak lagi diperlukan untuk menghalang pendedahan maklumat sensitif yang tidak perlu dan untuk mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak.</p> <p>Apabila memadam maklumat mengenai sistem, aplikasi dan perkhidmatan, perkara berikut harus dipertimbangkan:</p> <p>Kaedah pemadaman (cth., timpa elektronik atau pemadaman kriptografi) hendaklah dipilih mengikut keperluan perniagaan dan pertimbangan undang-undang dan peraturan yang berkaitan.</p> <p>Keputusan pemadaman hendaklah direkodkan sebagai bukti.</p> <ul style="list-style-type: none"> <li>• Apabila menggunakan pembekal perkhidmatan, bukti pemadaman maklumat harus diperoleh daripada mereka</li> <li>• Menggunakan perisian pemadaman selamat yang diluluskan untuk memadam maklumat secara kekal bagi membantu memastikan maklumat tidak dapat dipulihkan dengan menggunakan alat pemulihan pakar atau forensik.</li> <li>• Menggunakan pembekal yang diluluskan dan diperakui bagi perkhidmatan pelupusan selamat.</li> <li>• Menggunakan mekanisme pelupusan yang sesuai untuk jenis media storan yang dilupuskan</li> </ul>	Semua

1

1

0

5

'Data Deletion' ##8.10

NO	PENERANGAN	TINDAKAN
01	<p>Maklumat harus dipadamkan apabila tidak lagi diperlukan untuk menghalang pendedahan maklumat sensitif yang tidak perlu dan untuk mematuhi keperluan undang-undang, berkanun, peraturan dan kontrak.</p> <p>Apabila memadam maklumat mengenai sistem, aplikasi dan perkhidmatan, perkara berikut harus dipertimbangkan:</p> <p>Kaedah pemadaman (cth., timpa elektronik atau pemadaman kriptografi) hendaklah dipilih mengikut keperluan perniagaan dan pertimbangan undang-undang dan peraturan yang berkaitan.</p> <p>Keputusan pemadaman hendaklah direkodkan sebagai bukti.</p> <ul style="list-style-type: none"> <li>• Apabila menggunakan pembekal perkhidmatan, bukti pemadaman maklumat harus diperoleh daripada mereka</li> <li>• Menggunakan perisian pemadaman selamat yang diluluskan untuk memadam maklumat secara kekal bagi membantu memastikan maklumat tidak dapat dipulihkan dengan menggunakan alat pemulihan pakar atau forensik.</li> <li>• Menggunakan pembekal yang diluluskan dan diperakui bagi perkhidmatan pelupusan selamat.</li> <li>• Menggunakan mekanisme pelupusan yang sesuai untuk jenis media storan yang dilupuskan</li> </ul>	Semua

1

1

0

5

**Penopengan Data ##8.11**

NO	PENERANGAN	TINDAKAN
<b>01</b>	<p>Penopengan data ialah proses mengubah suai data sensitif supaya ia tidak bernilai atau sedikit kepada penyerang sementara masih boleh digunakan oleh perisian atau kakitangan atau sistem yang diberi kuasa.</p> <p>Masking digunakan pada medan data untuk melindungi data yang diklasifikasikan sebagai maklumat pengenalan peribadi, data peribadi sensitif atau data sensitif komersial.</p> <p>Kawalan yang boleh digunakan untuk penyamaran data termasuk:</p> <ul style="list-style-type: none"> <li>• Penyulitan data</li> <li>• Membatalkan atau memadam aksara untuk menghalang pengguna yang tidak dibenarkan daripada melihat mesej penuh</li> <li>• Mengubah nombor dan Tarikh</li> <li>• Penggantian dengan menukar satu nilai kepada nilai lain untuk menyembunyikan data sensitif</li> <li>• Data pencincangan, yang mengubah data secara tidak dapat diubah menjadi nilai atau kunci unik yang mewakili nilai asal</li> </ul>	Semua

1

1

0

5

**Perlindungan Ketirisan Maklumat Elektronik – DLP  
(MAMPU Web) ##8.12**

NO	PENERANGAN	TINDAKAN
01	<p>Pembendungan ketirisan maklumat ialah sebuah proses untuk mencegah dan mengesan pendedahan yang tidak dibenarkan dan pengestrakan maklumat daripada individu atau sistem. Langkah pencegahan sepatutnya digunakan kepada sistem, rangkaian dan lain lain perkakasan yang memproses, menyimpan atau menghantar informasi sensitif. Langkah ini sepatutnya menjadi gabungan polisi, proses dan peralatan teknikal.</p> <p>Contoh kawalan yang boleh digunakan :</p> <ul style="list-style-type: none"> <li>• Polisi dan proses untuk mengenalpasti dan mengklasifikasi maklumat untuk melindungi daripada ketirisan</li> <li>• Akses polisi kawalan</li> </ul> <p>Perkakasan teknikal untuk:</p> <ul style="list-style-type: none"> <li>• Memantau potensi punca ketirisan maklumat seperti email, pindahan fail, peranti mudah alih, dan peranti storan mudah alih</li> <li>• Mengenal pasti dan memantau maklumat sensitif pada risiko pendedahan yang tidak dibenarkan</li> <li>• Mengesan pendedahan maklumat sensitif</li> <li>• Menyekat tindakan pengguna atau transmisi rangkaian yang mendedahkan maklumat sensitif</li> </ul>	Semua

1

1

0

5

Pemantauan Aktiviti ##(8.16)

NO	PENERANGAN	TINDAKAN
01	<p>Pemantauan sistem ialah amalan memantau rangkaian, sistem dan aplikasi untuk mengesan tingkah laku anomali dan kemungkinan insiden keselamatan maklumat.</p> <p>Pemantauan hendaklah berterusan menggunakan alat pemantauan dalam masa nyata atau dalam selang masa berkala, tertakluk kepada keperluan dan keupayaan organisasi. Prosedur harus disediakan untuk bertindak balas tepat pada masanya untuk meminimumkan kesan kejadian buruk.</p> <p>Perkara berikut perlu dipertimbangkan untuk dimasukkan ke dalam sistem pemantauan:</p> <ul style="list-style-type: none"> <li>• Rangkaian, sistem dan aplikasi keluar dan masuk</li> <li>• Akses kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal</li> <li>• Sistem dan konfigurasi rangkaian peringkat kritikal atau pentadbir</li> <li>• Log daripada alatan keselamatan g., antivirus, Sistem Pengesanan Pencerobohan (IDS), Sistem Pencegahan Pencerobohan (IPS), penapis web, tembok api, Pencegahan Kebocoran Data (DLP), Alat Pengurusan Acara Maklumat Keselamatan (SIEM).</li> <li>• Log peristiwa yang berkaitan dengan sistem dan rangkaian</li> </ul>	Semua

1

1

0

5

Penapisan Web ##(8.23)

NO	PENERANGAN	TINDAKAN
01	<p>Penapisan web ialah teknologi yang menghalang pengguna daripada melihat URL atau tapak web tertentu dengan menghalang pelayar mereka daripada memuatkan halaman daripada tapak ini. Penapis web boleh menyampaikan pelbagai penyelesaian untuk kegunaan peribadi atau perusahaan.</p> <p>Organisasi harus mempertimbangkan untuk menyekat akses kepada jenis tapak web berikut:</p> <ul style="list-style-type: none"> <li>• Tapak web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perniagaan yang sah, seperti perkhidmatan perkongsian fail.</li> <li>• Tapak web yang diketahui atau disyaki berniat jahat, contohnya, yang mengedarkan kandungan perisian hasad atau pancingan data.</li> <li>• Pelayan perintah dan kawalan.</li> <li>• Tapak web berkongsi kandungan haram.</li> </ul>	Semua

1

1

0

5

**Pengekodaan Selamat ##(8.28)**

NO

PENERANGAN

TINDAKAN

01

Prinsip pengekodaan selamat hendaklah digunakan pada pembangunan perisian untuk memastikan perisian ditulis dengan selamat sekali gus mengurangkan bilangan potensi kelemahan keselamatan maklumat dalam perisian.

Contoh Kawalan:

- Wujudkan proses seluruh organisasi untuk menyediakan tadbir urus yang baik untuk pengekodaan selamat.
- Konfigurasikan alatan pembangunan, seperti persekitaran pembangunan bersepadu (IDE), untuk membantu menguatkuasakan penciptaan kod selamat.
- Penyelenggaraan dan penggunaan alat pembangunan yang dikemas kini (cth., penyusun).
- Latihan pemaju secara bertulis selamat
- Reka bentuk dan seni bina yang selamat, termasuk ancaman
- Penggunaan piawaian pengekodaan selamat dan di mana relevan mewajibkannya
- Penggunaan persekitaran terkawal untuk pembangunan.
- Amalan pengekodaan selamat khusus untuk bahasa dan teknik pengaturcaraan.
- Menggunakan pengaturcaraan berstruktur.
- Melarang penggunaan teknik reka bentuk yang tidak selamat (cth., penggunaan kata laluan berkod keras, sampel kod yang tidak diluluskan dan perkhidmatan web yang tidak disahkan).

Semua

# GLOSARI

GLOSARI	PENERANGAN
<b>Antivirus</b>	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM untuk sebarang kemungkinan adanya virus.
<b>Aset ICT</b>	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
<b>Backup</b>	Proses penduaan sesuatu dokumen atau maklumat.
<b>Bandwidth</b>	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
<b>BCP</b>	Business Continuity Planning Pelan tindakan untuk merancang aktiviti-aktiviti kesinambungan perkhidmatan.
<b>CERT</b>	Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
<b>CIO</b>	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
<b>Denial of service</b>	Halangan pemberian perkhidmatan.
<b>Downloading</b>	Aktiviti muat-turun sesuatu perisian.
<b>Encryption</b>	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
<b>Firewall</b>	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi keduanya.
<b>Forgery</b>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft / espionage), penipuan(hoaxes).
<b>GCERT</b>	Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
<b>Hard disk</b>	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
<b>Hub</b>	Peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
<b>ICT</b>	Information and Communication Technology. (Teknologi Maklumat dan Komunikasi).
<b>ICTSO</b>	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
<b>Internet</b>	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
<b>Internet Gateway</b>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.

# GLOSARI

GLOSARI	PENERANGAN
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	Log-out komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
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 Kementerian.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan 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 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.

**DISEDIAKAN :**  
**UNIT TEKNOLOGI MAKLUMAT,**  
**BAHAGIAN KORPORAT DAN PEMBANGUNAN,**  
**LEMBAGA PELABUHAN KUANTAN.**



