DASAR KESELAMATAN ICT

PEJABAT DAERAH DAN TANAH SELAMA

Terbitan	:	2016 Pejabat Daerah Dan Tanah Selama
Telefon	:	05-8394963
Fax	:	05-8394044
Laman Web	:	https://pdtselama.perak.gov.my
Email	:	pdtselama@perak.gov.my
Pegawai Daerah	:	Tn. Kamarudin Bin Awang

©2013 Hakcipta terpelihara. Tidak dibenar mengeluar ulang mana-mana bahagian isi kandungan daripada buku ini termasuk artikel, borang dan foto dalam apa jua bentuk dan cara sekalipun sama ada fotokopi, mekanik, rakaman, cetakan, elektronik atau cara-cara lain tanpa terlebih dahulu mendapat izin bertulis daripada PEJABAT DAERAH DAN TANAH SELAMA berhak untuk mengubah. Menukar atau membekal dokumen tanpa hebahan notis awalan terlebih dahulu.

Pejabat Daerah Dan Tanah Selama tidak akan menanggung sebarang kerugian, kerosakan diatas penggunaan dokumen atau dasar yang berkuatkuasa ini.

PENGHARGAAN

Assalammualaikum WBT dan selamat sejahtera.

Alhamdulillah, terlebih dahulu saya ingin mengucapkan tahniah kepada Unit Teknologi Maklumat (Unit ICT) dibawah Bahagian Khidmat Pengurusan (BKP) atas kejayaan menghasilkan Dasar Keselamatan ICT (DKICT) Pejabat Daerah & Tanah Selama (PDTS) yang akan menjadi rujukan oleh warga kerja jabatan ini.

Adalah menjadi hasrat kerajaan negeri untuk meningkatkan keberkesanan dan kecekapan sistem penyampaian melalui penggunaan ICT. Selaras dengan hasrat ini, Pejabat Daerah & Tanah Selama telah menjadikan teknologi ICT sebagai salah satu faktor dalam meningkatkan kecekapan dan kualiti penyampaian perkhidmatan urusan pentadbiran daerah dan tanah kepada pelanggan. Pelbagai saluran interaktif berasaskan teknologi ICT disediakan seperti aplikasi secara online, perkhidmatan laman web jabatan,aplikasi dalaman secara *Local Area Network (LAN)* di samping perkhidmatan sedia ada yang juga berasaskan ICT.

Sejajar dengan kemajuan teknologi ICT yang berkembang dengan begitu pesat dan canggih pada hari ini, pengguna ICT tidak dapat lari dari ancaman siber. Di antara bentuk ancaman yang kerap berlaku adalah seperti pencerobohan, pemalsuan (forgery), penghalangan penyampaian perkhidmatan (Denial Of Service), spam, kod-kod jahat (malicious code), serangan penggodam (hackers) dan pelbagai bentuk ancaman lain yang juga berkembang seiring dengan kemajuan teknologi.

Bagi mengimbangi perkembangan bentuk ancaman ini,adalah penting bagi warga Pejabat Daerah & Tanah Selama selaku pengguna ICT memahami dan mengetahui kaedah serta prodesur yang telah ditetapkan dalam menggunakan sumber ICT sedia ada seperti peralatan, perisian, dan aplikasi ICT secara berhemah yang seterusnya dapat mengurangkan risiko terdedah kepada pelbagai bentuk ancaman siber.

Sebagai memenuhi hasrat ini, penerbitan dokumen Dasar Keselamatan ICT ini diharap dapat dijadikan panduan oleh semua warga kerja Pejabat Daerah & Tanah Selama di samping memberi pendedahan mengenai kaedah penggunaan ICT yang selamat dan bahaya ancaman siber terhadap operasi jabatan.

Akhir kata, saya menyeru kepada semua warga Pejabat Daerah & Tanah Selama agar dapat menggunakan sumber ICT yang dibekalkan dengan bijak dan berhemah serta mematuhi peraturan serta arahan keselamatan ICT yang terkandung dalam DKICT PDTS.

Terima Kasih,

TN. KAMARUDIN BIN AWANG

	KANDUNGAN		MUKA SURAT
	PENGENALAN		1
1.	PEMBANGUNAN DAN PENYELENGGARAAN DASAR		3
	1.1 Dasar Keselamatan ICT		
		1.1.1 Pelaksanaan Dasar	
		1.1.2 Penyebaran Dasar 1.1.3 Penyelengaraan Dasar	
		1.1.4 Pengecualian Dasar	
2.	ORGANISASI KESELAMATAN		5
	2.1 Infrastruktur Organisasi Keselamatan		
		2.1.1 Pengarah	
		2.1.2 Ketua Pegawai Maklumat (CIO)	
		2.1.3 Pegawai Keselamatan ICT (ICTSO)	
		2.1.4 Pengurus Komputer	
		2.1.5 Pentadbir Sistem ICT	
		2.1.6 Pengguna	
	2.2 Pihak Ketiga		
		2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
3.	KAWALAN DAN PENGELASAN ASET		10
	3.1 Akauntabiliti Aset		
		3.1.1 Inventori Aset	
	3.2 Pengelasan dan Pengendalian Maklumat		
		3.2.1 Pengelasan Maklumat	

	KANDUNGAN		MUKA SURAT
		3.2.2 Pengendalian Maklumat	
4.	KESELAMATAN SUMBER MANUSIA		12
	4.1 Keselamatan ICT Dalam Tugas Harian		
		4.1.1 Tanggungjawab Keselamatan	
		4.1.2 Terma dan Syarat Perkhidmatan	
		4.1.3 Perakuan Akta Rahsia Rasmi	
	4.2 Menangani Insiden Keselamatan ICT		
		4.2.1 Pelaporan Insiden	
	4.3 Pendidikan		
		4.3.1 Program Kesedaran Keselamatan ICT	
	4.4 Tindakan Tatatertib		
		4.4.1 Pelanggaran Dasar	
5.	KESELAMATAN FIZIKAL		15
	5.1 Keselamatan Kawasan		
		5.1.1 Perimeter Keselamatan Fizikal	
		5.1.2 Kawalan MasukFizikal	
		5.1.3 Kawasan Larangan	
	5.2 Keselamatan Peralatan		
		5.2.1 Perkakasan	
		5.2.2 Dokumen	
		5.2.3 Media Storan	

	KANDUNGAN		MUKA SURAT
		5.2.4 Kabel	
		5.2.5 Penyelenggaraan	
		5.2.6 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	
		5.2.7 Peralatan Di Luar Premis	
		5.2.8 Pelupusan	
		5.2.9 Clear Desk dan Clear Screen	
	5.3 Keselamatan Persekitaran		
		5.3.1 Kawalan Persekitaran	
		5.3.2 Bekalan Kuasa	
		5.3.3 Prosedur Kecemasan	
6.	PENGURUSAN OPERASI DAN KOMUNIKASI		21
	6.1 Pengurusan Prosedur Operasi		
		6.1.1. Pengendalian Prosedur	
		6.1.2. Kawalan Perubahan	
		6.1.3. Prosedur Pengurusan Insiden	
	6.2. Perancangan dan Penerimaan Sistem		
		6.2.1. Perancangan Kapasiti	
		6.2.2. Penerimaan Sistem	
	6.3. Perisian Berbahaya		
		6.3.1. Perlindungan dari Perisian Berbahaya	
	6.4. Housekeeping		

	KANDUNGAN		MUKA SURAT
		6.4.1. Penduaan	
		6.4.2. Sistem Log	
	6.5. Pengurusan Rangkaian		
		6.5.1. Kawalan Infrastruktur Rangkaian	
	6.6. Pengurusan Media		
		6.6.1. Penghantaran dan Pemindahan	
		6.6.2. Prosedur Pengendalian Media	
		6.6.3. Keselamatan Sistem Dokumentasi	
	6.7. Keselamatan Komunikasi		
		6.7.1. Internet	
		6.7.2. Mel Elektronik	
7.	KAWALAN CAPAIAN		28
	7.1 Keselamatan ICT Dalam Tugaan Harian		
		7.1.1 Keperluan Dasar	
	7.2 Pengurusan Capaian Pengguna		
		7.2.1 Akaun Pengguna	
		7.2.2 Jejak Audit	
	7.3 Kawalan Capaian Sistem dan Aplikasi		
		7.3.1 Sistem Maklumat dan Aplikasi	
	7.4 Peralatan Komputer Mudah alih		
		7.4.1 Penggunaan Peralatan Komputer Mudah Alih	

	KANDUNGAN	MUKA SURAT
8.	PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	31
	8.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
	8.1.1 Keperluan Keselamatan	
	8.2 Kriptografi	
	8.2.1 Penyulitan	
	8.2.2 Tandatangan Digital	
	8.2.3 Pengurusan Kunci	
	8.3 Fail Sistem	
	8.3.1 Kawalan Fail Sistem	
	8.4 Pembangunan dan Proses Sokongan	
	8.4.1 Kawalan Perubahan	
9.	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	34
	9.1 Dasar Kesinambungan Perkhidmatan	
	9.1.1 Pelan Kesinambungan Perkhidmatan	
10.	PEMATUHAN	36
	10.1 Pematuhan dan Keperluan Perundangan	
	10.1.1 Pematuhan Dasar	
	10.1.2 Keperluan Perundangan	
	APPENDIK 1 : Surat Akuan Pematuhan	38

PENGENALAN

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

OBJEKTIF

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

SKOP

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT PDTS dan perlu dipatuhi adalah seperti berikut:

a) **Akses atas dasar perlu mengetahui**
Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut;

b) **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 mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas

c) **Akauntabiliti**
Semua pengguna adalah bertanggunjawab ke atas semua tindakannya terhadap aset ICT PDTS;

d) **Pengasingan**
Tugas mewujud, memadam, kemaskini, 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 operasi dan rangkaian;

e) **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamtan. Ia melibatkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f) **Pematuhan**

Dasar keselamatan ICT PDTS hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g) **Pemulihan**

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

h) **Saling Bergantungan**

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

PEMBANGUNAN
DAN
PENYELENGGARAAN DASAR

PEJABAT DAERAH & TANAH
SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	3

Perkara 01 - Pembangunan Dan Penyelenggaraan Dasar

Dasar Keselamatan ICT		
DM-010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Penolong Pegawai Daerah Pejabat Daerah & Tanah Selama dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan Penolong Pegawai Daerah.	**Ketua Penolong Pegawai Daerah**
DM-010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna PDTS (termasuk kakitangan di pejabat-pejabat penghulu mukim, pembekal, pakar runding dll.)	**ICTSO**
DM-010103 Penyelenggaraan Dasar		
	Dasar Keselamatan ICT PDTS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT PDTS : a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu ICT (JPICT); c) Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	**ICTSO**
DM-010104 Pengecualian Dasar		
	Dasar Keselamatan ICT PDTS adalah terpakai kepada semua pengguna ICT PDTS dan tiada pengecualian diberikan.	**Semua**

ORGANISASI KESELAMATAN

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	5

Perkara 02 – Organisasi Keselamatan

Infrastruktur Organisasi Keselamatan		
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
DM-020101 Pegawai Daerah		
	Peranan dan tanggungjawab Pengarah adalah seperti berikut : a) Memastikan semua pengguna memahami peruntukan- peruntukan dibawah Dasar Keselamatan; b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PDTS; c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlidungan keselamatan) adalah mencukupi; dan d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PDTS.	**Pegawai Daerah**
DM-020102 Ketua Pegawai Maklumat (CIO)		
	KPPD PDTS adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut : a. Membantu Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; dan c. Membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	**CIO**
DM-020103 Pegawai Keselamatan ICT (ICTSO)		

	Penolong Pegawai Daerah PDTS adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Menguruskan keseluruhan program-program keselamatan ICT PDTS; b) Menguatkuasakan keseluruhan keselamatan ICT PDTS; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT PDTS kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT PDTS; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas	**ICTSO**

	pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera; j) Memperakui proses pengambilan tindakan tatatertib ke 0atas pengguna yang melanggar Dasar Keselamatan ICT PDTLMS; dan k) Menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
DM-020104 Pengurus Komputer		
	Penolong Pegawai Daerah (BKP) adalah merupakan Pengurus Komputer PDTS. Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut : a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PDTS; b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PDTS; c) Menentukan kawalan akses semua pengguna terhadap aset ICT PDTS; d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PDTS.	**Pengurus Komputer**
DM-020105 Pentadbir Sistem ICT		

	Juruteknik Komputer adalah merupakan Pentadbir Sistem ICT PDTS. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut : a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti,	**Pentadbir Sistem ICT**

	bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Kesematan ICT PDTS; c) Memantau aktiviti capaian harian pengguna; d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menyimpan dan menganalisis rekod jejak audit; dan f) Menyediakan laporan aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
DM-020106 Pengguna		

	Peranan dan tanggungjawab Pengguna adalah seperti berikut : a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT PDTS; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Lulus tapisan keselamatan; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat PDTS; e) Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia 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 ketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g) Menghadiri program-program kesedaran mengenai	**Pengguna**

	keselamatan ICT; dan h) Menandatangani surat akuan pematuhan Dasar Keselamatan ICT PDTS.	
Pihak Ketiga **Objektif :** Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
DM-020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga		
	Akses kepada aset ICT PDTS perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. a) Dasar Keselamatan ICT PDTS; b) Tapisan Keselamatan; c) Perakuan Akta Rahsia Rasmi 1972; dan d) Hak Harta Intelek. Nota 1 : Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan juga boleh dirujuk.	**CIO, ICTSO, Pengurus Komputer, Pentadbir Sistem ICT dan Pihak Ketiga**

KAWALAN
DAN
PENGELASAN ASET

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	10

Perkara 03 - Kawalan dan Pengelasan Aset

<table>
<tr><td colspan="3">Akauntabiliti Aset
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset PDTLMS.</td></tr>
<tr><td colspan="3">DM-030101 Inventori Aset</td></tr>
<tr><td></td><td>Semua aset ICT PDTS hendaklah direkodkan.

Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.</td><td>Ketua Penolong Pegawai Daerah</td></tr>
<tr><td colspan="3">Pengelasan dan Pengendalian Maklumat
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.</td></tr>
<tr><td colspan="3">DM-030201 Pengelasan Maklumat</td></tr>
<tr><td></td><td>Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :

a. Rahsia Besar;
b. Rahsia;
c. Sulit; atau
d. Terhad</td><td>CIO</td></tr>
<tr><td colspan="3">DM-030202 Pengendalian Maklumat</td></tr>
</table>

	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dsb g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	**Semua**

KESELAMATAN SUMBER MANUSIA

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	**13**

Perkara 04 – Keselamatan Sumber Manusia

Keselamatan ICT Dalam Tugas Harian **Objektif :** Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT PDTS.		
DM-040101 Tanggungjawab Keselamatan		
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	**Semua**
DM-040102 Terma dan Syarat Perkhidmatan		
	Semua warga PDTS yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	**Semua**
DM-040103 Perakuan Akta Rahsia Rasmi		
	Warga PDTS yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	**Semua**
Menangani Insiden Keselamatan ICT **Objektif :** Meminimumkan kesan insiden keselamatan ICT.		
DM-040201 Pelaporan Insiden		
	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 hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota 2 : Pekeliling am Bilangan 1 Tahun 2001 bertajuk „Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk.	**Semua**
Pendidikan **Objektif:** Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
DM-040301 Program Kesedaran Keselamatan ICT		

	Setiap pengguna di PDTS perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT PDTS.	**ICTSO**
Tindakan Tatatertib **Objektif :** Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT PDTS.		
DM-040401 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT PDTS akan dikenakan tindakan tatatertib.	**Semua**

KESELAMATAN FIZIKAL

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	**15**

Perkara 05 – Keselamatan Fizikal

Keselamatan Kawasan

Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

DM-050101 Perimeter Keselamatan Fizikal

	Keselamatan fizikal adalah tujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a) Kawasan keselamatan fizikal hendahklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c) Memperkukuhkan dinding dan siling; d) Memasang alat penggera atau kamera; e) Menghadkan jalan keluar masuk; f) Mengadakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan h) Mewujudkan perkhidmatan kawalan keselamatan.	**Pejabat Ketua Pegawai Keselamatan Dalam Negeri, CIO dan ICTSO**

DM-050102 Kawalan Masuk Fizikal

	a) Setiap penguna PDTS hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c) Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d) Setiap pelawat hendaklah mendaftar di pintu utama bangunan Pejabat Daerah & Tanah SELAMA (PDTS) terlebih dahulu; e) Kehilangan pas mestilah dilaporkan dengan segera; f) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT PDTS.	**Semua dan pelawat**

DM-050103 Kawasan Larangan

	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di PDTS adalah bilik Ketua Penolong Pegawai Daerah, bilik Penolong Pegawai Daerah, bilik server, bilik Kebal. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja: a) Secara umumnya peralatan ICT hendaklah dijaga dengan baik supaya boleh digunakan bila perlu; b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka	**Semua**

	hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c) Semua pengguna peralatan yang melibatkan penghantaran, kemaskini dan menghapuskan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	
Keselamatan Peralatan **Objektif :** Melindungi peralatan dan maklumat.		
DM-050201 Perkakasan		
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu : a) Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan semurna; b) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	**Semua**
DM-050202 Dokumen		
	Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c) Menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan d) Memastikan dokumen yang mengandungi bahan atau maklumat sensitive diambil segera dari pencetak.	**Semua**
DM-050203 Media Storan		
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat : a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d) Pergerakan media storan hendaklah direkodkan.	**Semua**
DM-050204 Kabel		

	Kabel komputer hendaklah dilindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan c) Melindungi laluan pemasangan kabel sepenuhnya.	**UICT dan ICTSO**
DM-050205 Penyelenggaraan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b) Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c) Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah bahagian berkenaan	**Semua**
DM-050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat		
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan : a) Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuaan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	**Semua**
DM-050207 Peralatan Di Luar Premis		
	Bagi perkakasan yang dibawa keluar dari premis PDTS, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan PDTS : a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Peyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian	**Semua**
DM-050208 Pelupusan		
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PDTS : a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah	**Semua**

	membuat penduaan; dan c) Maklumat lanjut pelupusan bolehlah dirujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer".	
DM-050209 Clear Desk dan Clear Screen		
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya : a) Gunakan kemudahan password screen saver atau log keluar apabila meninggalkan computer; dan b) Bahan-bahan sensitive hendaklah disimpan dalam laci atau cabinet fail yang berkunci.	**Semua**
Objektif : Melindungi aset ICT PDTS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
DM-050301 Kawalan Persekitaran		
	Bagi menghindari kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Dalam Negeri. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil : a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer, ruang atur pejabat dan sebagainya) dengan teliti; 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; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	**Semua**
DM-050302 Bekalan Kuasa		
	a) Semua Peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;	**UCT, ICTSO**

	b) Peralatan sokongan seperti UPS (Uninterruptable Power Supply) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara jadual.	
DM-050303 Prosedur Kecemasan		
	a) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.	Semua

PENGURUSAN OPERASI DAN KOMUNIKASI

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	**21**

Perkara 06 – Pengurusan Operasi dan komunikasi

Pengurusan Prosedur Operasi **Objektif:** Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.		
DM-060101 Pengendalian Prosedur		
	b) Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; c) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan d) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	**Semua**
DM-060102 Kawalan Perubahan		
	a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan menpunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama asa sengaja atau pun tidak.	**Semua**
DM-060103 Prosedur Pengurusan Insiden		

	Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut : a) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b) Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c) Menyimpan jejak audit dan memelihara bahan bukti; dan d) Menyediakan tindakan pemulihan segera.	**JPICT PDTS, ICTSO**

Perancangan dan Penerimaan Sistem

Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

DM-060201 Perancangan Kapasiti

	a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**Pentadbir Sistem ICT, ICTSO**

DM-060202 Penerimaan Sistem

	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah mematuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**Pentadbir Sistem ICT, ICTSO**

Perisian Berbahaya

Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan Trojan.

DM-060301 Perlindungan dari Perisian Berbahaya

	a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan Intrusion Detection System (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (pindaan) Tahun 1997; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini pattern antivirus setiap minggu; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan balik sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	**Semua**

Housekeeping **Objektif :** Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.		
DM-060401 Penduaan		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di off site. a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi baru; b) Membuat salinan penduaan ke atas semua data maklumat mengikut keperluan operasi; dan c) Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	**Semua**
DM-060402 Sistem Log		
	a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang meyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktivit tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	**UICT**
Pengurusan Rangkaian **Objektif :** Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
DM-060501 Kawalan Infrastruktur Rangkaian		
	Infrasruktur Rangkaian mestilah di kawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :- a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan dilokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan kongfigurasi; e) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikongfigurasi oleh pentadbir	**UICT**

	sistem; f) Semua Trafik keluar masuk hendaklah melalui firewall dibawah kawalan PDTS	

	g) Semua Sniffer atau network analyzer adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian Intrusion Detection System (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PDTS; i) Memasang Web Content Filter pada Internet Gateway untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Pengguna Internet Mel Elektronik di Agensi-Agensi Kerajaan"; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan PDTS hendaklah mendapat kebenaran ICTSO; k) Semua pengguna hanya dibenarkan menggunakan rangkaian PDTS sahaja. Penggunaan modem adalah dilarang sama sekali;dan l) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
Pengurusan Media **Objektif :** Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.		
DM-060601 Penghantaran dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	**Semua**
DM-060602 Prosedur Pengendalian Media		
	a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media ditempat yang selamat; dan f) Media yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.	**Semua**
DM-060603 Keselamatan Sistem Dokumentasi		

	a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri- ciri keselamatan; b) Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	**Pentadbir sistem ICT, ICTSO**

Keselamatan Komunikasi		
Objektif : Melindungi aset ICT melalui sistem komunikasi yang selamat.		
DM-060701 Internet		
	a) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b) Bahan yang diperolehi dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c) Bahan rasmi disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hakcipta terpelihara; e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PDTLMS; f) 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 Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peruntukan yang telah ditetapkan; dan g) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Petadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan".	**Semua**
DM-060702 Mel Elektronik		

	a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh PDTS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang berkongsi bersama adalah dilarang; b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PDTS; c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e- mel rasmi dan pastikan alamat e-mel penerima adalah betul; e) Penggunaan dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) Megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i) E-mel yang tidak penting dan tidak menpunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;	**Semua**

	j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan k) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Petadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan".	

KAWALAN CAPAIAN

PEJABAT DAERAH & TANAH SELAMA

Perkara 07 – Kawalan Capaian

Keselamatan ICT Dalam Tugas Harian **Objektif :** Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT PDTS.		
DM-070101 Keperluan Dasar		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.	**UICT, ICTSO**
Pengurusan Capaian Pengguna **Objektif :** Mengawal capaian pengguna ke atas aset ICT PDTS.		
DM-070201 Akaun Pengguna		
	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 diperuntukan oleh jabatan sahaja boleh digunakan; b) Akaun penguna mestilah unik; c) Akuan pengguna yang di wujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap pencapaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau yang dikongsi bersama adalah dilarang; dan f) Pentadbir sistem ICT boleh membekukan atau menamatkan akaun pengguna atas sebab-sebab tertentu: - i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	**Semua**
DM-070202 Jejak Audit		
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi : a) Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan	**Pentadbir Sistem ICT**

	c) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
Kawalan Capaian Sistem dan Aplikasi **Objektif :** Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
DM-070301 Sistem Maklumat dan Aplikasi		
	Capaian sistem dan aplikasi di PDTS adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah- langkah berikut hendaklah dipatuhi : a) Penggunaan hanya boleh menggunakan sistem maklumat dan apliksai yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	**Pentadbir Sistem ICT, ICTSO**
Peralatan Komputer Mudah Alih **Objektif :** Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
DM-070401 Penggunaan Peralatan Komputer Mudah Alih		
	a) Merekod aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan b) Komputer mudah alih hendaklah disimpan dan dikunci di tempat selamat apabila tidak digunakan	**Semua**

PEMBANGUNAN
DAN
PENYELENGGARAAN SISTEM

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	**31**

Perkara 08 - Pembangunan Dan Penyelenggaraan Sistem

Keselamatan Dalam Membangunkan Sistem dan Aplikasi **Objektif :** Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
DM-080101 Keperluan Keselamatan		
	a) Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem output untuk memastikan data yang telah diproses adalah tepat; dan c) Sebaik-baiknya semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Pemilik Sistem, Pentadbir Sistem ICT, ICTSO**
Kriptografi **Objektif :** Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
DM-080201 Penyulitan		
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	**Semua**
DM-080202 Tandatangan Digital		
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	**Semua**
DM-080203 Pengurusan Kunci		
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah , di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	**Semua**
Fail Sistem **Objektif :** Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
DM-080301 Kawalan fail Sistem		
	a) Proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan	**Pentadbir Sistem ICT**

	d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistic, pemulihan dan keselamatan.	
Pembangunan dan Proses Sokongan **Objektif :** Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
DM-080401 Kawalan Perubahan		
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai.	**Pentadbir Sistem ICT**

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PEJABAT DAERAH & TANAH SELAMA

RUJUKAN	REVERSI	TARIKH	M/SURAT
DKICT PDTS	Versi 1.0	5 Januari 2016	**34**

Perkara 09 – Pengurusan Kesinambungan Perkhidmatan

<table>
<tr><td colspan="3">Dasar Kesinambungan Perkhidmatan
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.</td></tr>
<tr><td colspan="3">DM-090101 Pelan Kesinambungan Perkhidmatan</td></tr>
<tr><td></td><td>Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian :

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 penduaan; dan
f) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.</td><td>ICTSO</td></tr>
</table>

PEMATUHAN

PEJABAT DAERAH & TANAH SELAMA

Perkara 10 – Pematuhan

<table>
<tr><td colspan="3">Pematuhan dan Keperluan Perundangan
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT PDTS.</td></tr>
<tr><td colspan="3">DM-100101 Pematuhan Dasar</td></tr>
<tr><td></td><td>Setiap pengguna di PDTS hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT PDTS dan undang-undang atau peraturan – peraturan lain yang berkaitan yang berkuat kuasa.

Semua aset ICT di PDTS termasuk maklumat yang disimpan di dalamnya adalah hak milik kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.</td><td>Semua</td></tr>
<tr><td colspan="3">DM-100102 Keperluan Perundangan</td></tr>
<tr><td></td><td>Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PDTS:
a) Arahan Keselamatan;
b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Keselamatan maklumat Sektor Awam;
g) Akta Tandatangan Digital 1997;
h) Akta Jenayah Komputer 1997;
i) Akta Hakcipta (Pindaan) Tahun 1997; dan
j) Akta Komunikasi dan Multimedia 1998.</td><td>Semua</td></tr>
</table>

APPENDIK 1
SURAT AKUAN PEMATUHAN

PEJABAT DAERAH & TANAH SELAMA

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT, PDTS

Nama (Huruf Besar) : ……………………………………………….

No.KadPengenalan: ……………………………………………….

Jawatan : ……………………………………………….

Bahagian : ……………………………………………….

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT, PDTS; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan :

…………………………………………

Tarikh : ………………………………

Pengesahan Pegawai Keselamatan ICT

…………………………………………………….
( )
b.p : Ketua Penolong Pegawai Daerah
Pejabat Daerah & Tanah Selama
Tarikh :……………………………