2018

DKICT

DASAR KESELAMATAN ICT

PEJABAT DAERAH & TANAH MANJUNG

Terbitan	:	2018 @ Pejabat Daerah dan Tanah Manjung
Telefon	:	05-688 1120 / 6270 / 2117
Fax	:	05-688 2106
Laman Web	:	http://pdtmanjung.perak.gov.my
Emel	:	pdtmanjung@perak.gov.my pdtmanjung@gmail.com
Pegawai Daerah	:	Ybhg. Dato' Mohamad Fariz bin Mohamad Hanip, D.P.M.P, A.M.P

PENGHARGAAN

Assalammualaikum WBT, selamat sejahtera dan salam Negaraku.

Alhamdulillah, terlebih dahulu saya ingin mengucapkan tahniah kepada Unit Teknologi Maklumat di bawah Bahagian Khidmat Pengurusan (BKP) atas kejayaan menghasilkan **Dasar Keselamatan ICT (DKICT) Pejabat Daerah dan Tanah Manjung (PDTMJG) versi 1 / 2018** 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 dan Tanah Manjung 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 portal 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 dan Tanah Manjung 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 dan Tanah Manjung 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 dan Tanah Manjung agar dapat menggunakan sumber ICT yang dibekalkan dengan bijak dan berhemah serta mematuhi peraturan serta arahan keselamatan ICT yang terkandung dalam DKICT PDTMJG versi 1 / 2018.

Sekian, terima kasih.

.....

Ybhg. Dato' Mohamad Fariz bin Mohamad Hanip, **D.P.M.P, A.M.P**
Pegawai Daerah
Pejabat Daerah dan Tanah Manjung

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
1 Januari 2018	1.0	Mesyuarat Pengurusan Bilangan 1 / 2018	1 Januari 2018

JADUAL PINDAAN DOKUMEN

TARIKH	VERSI	BUTIRAN PINDAAN
Tiada	Tiada	Tiada

KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung diwujudkan untuk menjamin kesinambungan urusan Pejabat Daerah dan Tanah Manjung dengan meminimumkan kesan insiden keselamatan ICT.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

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

Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(i) Kerahsiaan
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan untuk diakses tanpa kebenaran;

(ii) Integriti
Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(iii) Tidak Boleh Disangkal
Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(iv) Kesahihan
Data dan maklumat hendaklah dijamin kesahihannya; dan

(v) Ketersediaan
Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;

(i) ancaman yang wujud akibat daripada kelemahan tersebut;

(ii) risiko yang mungkin timbul; dan

(iii) langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

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 Pejabat Daerah dan Tanah Manjung termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, muatturun, menyedia, muatnaik, berkongsi, menyimpan dan menggunakan aset ICT Pejabat Daerah dan Tanah Manjung.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung yang perlu dipatuhi adalah seperti berikut:

(i) 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;

(ii) 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;

(iii) Akauntabiliti

Semua pengguna adalah bertanggunjawab ke atas semua tindakannya terhadap aset ICT Pejabat Daerah dan Tanah Manjung;

(iv) 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;

(v) Pengauditan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti 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;

(vi) Pematuhan

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

(vii) 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

(viii) Saling Bergantungan

Setiap prinsip di atas adalah saling 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.

BIDANG 01

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

BIDANG 01 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101	**Dasar Keselamatan ICT**	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Pejabat Daerah dan Tanah Manjung dan perundangan yang berkaitan.		
010101	**Pelaksanaan Dasar**	**Tindakan**
	Pelaksanaan dasar ini akan dijalankan oleh Pegawai Daerah, Pejabat Daerah dan Tanah Manjung yang dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan semua Penolong Pegawai Daerah bagi setiap bahagian.	**Pengarah**
010102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna Pejabat Daerah dan Tanah Manjung (termasuk kakitangan di pejabat-pejabat penghulu mukim, pembekal, pakar runding dll.)	**ICTSO**
010103	**Penyelenggaraan Dasar**	
	Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur berhubung dengan penyelenggaraan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung : (a) Kenalpasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan mesyuarat JPICT;	**ICTSO**

	(c) Perubahan yang telah dipersetujui oleh JPICT akan dimaklumkan kepada semua pengguna; dan (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	
010104	**Pengecualian Dasar**	
	Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung adalah terpakai kepada semua pengguna ICT Pejabat Daerah dan Tanah Manjung dan tiada pengecualian diberikan.	**Semua**

BIDANG 02

ORGANISASI KESELAMATAN

BIDANG 02 – ORGANISASI KESELAMATAN

0201	**Infrastruktur Organisasi Dalaman**	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
020101	**Pengarah**	**Tindakan**
	Pegawai Daerah bagi Pejabat Daerah dan Tanah Manjung adalah merupakan Pengarah bagi keseluruhan DKICT. 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 Pejabat Daerah dan Tanah Manjung; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlidungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung; dan (e) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**Pengarah**

020102	**Ketua Pegawai Maklumat (CIO)**	
	Ketua Penolong Pegawai Daerah (Tanah) Pejabat Daerah dan Tanah Manjung 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; (c) Membangun dan menyelaraskan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan (d) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**CIO**

020103	Pegawai Keselamatan ICT (ICTSO)	Tindakan
	Penolong Pegawai Daerah (BKP) Pejabat Daerah dan Tanah Manjung adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Menguruskan keseluruhan program-program keselamatan ICT Pejabat Daerah dan Tanah Manjung; (b) Menguatkuasakan keseluruhan keselamatan ICT Pejabat Daerah dan Tanah Manjung; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas 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 atas pengguna yang melanggar Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung; (k) Menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan (l) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**ICTSO**

020104	Pengurus ICT	Tindakan
	Penolong Pegawai Teknologi Maklumat adalah merupakan Pengurus ICT Pejabat Daerah dan Tanah Manjung. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut : (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung; (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Pejabat Daerah dan Tanah Manjung; (c) Menentukan kawalan akses semua pengguna terhadap aset ICT Pejabat Daerah dan Tanah Manjung; (d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Pejabat Daerah dan Tanah Manjung; dan (f) Menandatangani SuratAkuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**Pengurus ICT**

020105	**Pentadbir Sistem ICT**	
	Penolong Pegawai Teknologi Maklumat dan **Juruteknik Komputer** adalah merupakan Pentadbir Sistem ICT Pejabat Daerah dan Tanah Manjung. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut : (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, 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 Keselamatan ICT Pejabat Daerah dan Tanah Manjung; (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; dan (g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**Pentadbir Sistem ICT**
	h) Pentadbir Sistem ICT yang berkenaan hendaklah menandatangani Surat Aku Janji Keselamatan SPTB seperti yang termaktub dalam Pekeliling Ketua Pengarah Tanah dan Galian Persekutuan Bilangan 1/2012. Contoh Surat Aku Janji Keselamatan SPTB adalah seperti di **LAMPIRAN B** dan hendaklah diserahkan kepada Pegawai Keselamatan SPTB untuk simpanan.	**Pegawai Keselamatan SPTB**

020106	Pengguna	Tindakan
	Peranan dan tanggungjawab **Pengguna** adalah seperti berikut : (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung; (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 Pejabat Daerah dan Tanah Manjung; (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; (vii) Menjaga kerahsiaan langkah keselamatan ICT dari ketahui umum. (f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (g) Menghadiri program kesedaran keselamatan ICT; dan (h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**.	**CIO**

	(i) Pengguna SPTB hendaklah menandatangani Surat Aku Janji Keselamatan SPTB seperti yang termaktub dalam Pekeliling Ketua Pengarah Tanah dan Galian Persekutuan Bilangan 1/2012. Contoh Surat Aku Janji Keselamatan SPTB adalah seperti di **LAMPIRAN B** dan hendaklah diserahkan kepada Pegawai Keselamatan SPTB untuk simpanan.	**Pegawai Keselamatan SPTB**
0202	**Pihak Ketiga**	
Objektif: Menjamin keselamatan semua asset ICT yang digunakan oleh pihak ketiga.		
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	**Tindakan**
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Akses kepada aset ICT Pejabat Daerah dan Tanah Manjung perlu berlandaskan kepada perjanjian kontrak; (b) Perkara - perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. (i) Dasar Keselamatan ICT PDTHP; (ii) Tapisan Keselamatan; (iii) Perakuan Akta Rahsia Rasmi 1972; dan (iv) Hak Harta Intelek. (c) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung seperti di **LAMPIRAN A**. 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, Pengurus ICT, Pentadbir Sistem ICT, Pihak Ketiga**

BIDANG 03

PENGURUSAN ASET

BIDANG 03 – PENGURUSAN ASET

0301	**Akauntabiliti Aset**	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset Pejabat Daerah dan Tanah Manjung.		
030101	**Inventori Aset ICT**	**Tindakan**
	Semua aset ICT Pejabat Daerah dan Tanah Manjung 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.	**Pentadbir Sistem, Semua**
0302	**Pengelasan dan Pengendalian Maklumat**	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
030201	**Pengelasan Maklumat**	
	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.	**CIO**

030202 Pengendalian Maklumat		
	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; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	**Semua**

BIDANG 04

KESELAMATAN SUMBER MANUSIA

BIDANG 04 – KESELAMATAN SUMBER MANUSIA

0401	**Keselamatan Sumber Manusia Dalam Tugas Harian**	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan Pejabat Daerah dan Tanah Manjung bahagian masing-masing, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga Pejabat Daerah dan Tanah Manjung hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.		
040101	**Sebelum Perkhidmatan**	**Tindakan**
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan bahagian serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**

040102	**Dalam Perkhidmatan**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Pejabat Daerah dan Tanah Manjung secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan / atau undang-undang ke atas pegawai dan kakitangan Pejabat Daerah dan Tanah Manjung serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan (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. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan, Pejabat Daerah dan Tanah Manjung.	**Semua**
040103	**Bertukar Atau Tamat Perkhidmatan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada bahagian mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh pentadbiran Pejabat Daerah dan Tanah Manjung dan / atau terma perkhidmatan.	**Semua**

BIDANG 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 05 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501	**Keselamatan Kawasan**	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.		
050101	**Kawalan Masuk Fizikal**	**Tindakan**
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang 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) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; (d) Memperkukuhkan dinding dan siling; (e) Memasang alat penggera atau kamera; (f) Menghadkan jalan keluar masuk; (g) Mengadakan kaunter kawalan; (h) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan (i) Mewujudkan perkhidmatan kawalan keselamatan.	**BKP, bahagian masing-masing**

050102	**Kawalan 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 Pejabat Daerah dan Tanah Manjung adalah bilik Pegawai Daerah, bilik-bilik Ketua Penolong Pegawai Daerah, bilik-bilik Penolong Pegawai Daerah, bilik server dan bilik kebal. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa dan diberi kebenaran 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 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.	**Semua**

0502	Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT Pejabat Daerah dan Tanah Manjung dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.		
050201	**Peralatan ICT**	**Tindakan**
	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 sempurna; (b) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (c) Peralatan ICT yang hendak dibawa keluar dari premis bahagian, perlulah mendapat kelulusan Ketua Bahagian dan direkodkan bagi tujuan pemantauan; (d) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan (e) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	**Semua**
050202	**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;	**Semua**

	(c) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan (d) Pergerakan media storan hendaklah direkodkan.	
050203	**Penyelenggaraan Perkakasan**	**Tindakan**
	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) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran Pengurus ICT.	**Semua**
050204	**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**

050205	Pelupusan Perkakasan	Tindakan
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Pejabat Daerah dan Tanah Manjung, PTG Perak, JKPTG, SUK Perak, dan ditempatkan di Pejabat Daerah dan Tanah Manjung. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal mengikut 1PP (Pekeliling Perbendaharaan) AM: Tatacara Pengurusan Aset Kerajaan dan lengkap supaya maklumat tidak terlepas dari kawalan Pejabat Daerah dan Tanah Manjung dan bahagian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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 membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindahmilik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan ditempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori; (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan	**Semua**

	(h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; (ii) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di Pejabat Daerah dan Tanah Manjung; (iii) Memindah keluar dari Pejabat Daerah dan Tanah Manjung mana-mana peralatan ICT yang hendak dilupuskan; (iv) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Unit Teknologi Maklumat atau Unit Aset, Bahagian Khidmat Pengurusan. (v) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti pendrive atau external hardisk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

0503	Keselamatan Persekitaran	
Objektif: Melindungi aset ICT Pejabat Daerah dan Tanah Manjung dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
050301	**Kawalan Persekitaran**	**Tindakan**
	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**

050302	Bekalan Kuasa	Tindakan
	Bekalan kuasa merupakan punca kuasa elektrik yang di bekalkan peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua Peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrikdan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (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.	**ICT, ICTSO**
050303	**Kabel**	
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan 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; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat. (e) Sebarang pemasangan serta penambahan kabel baru ke LAN hendaklah mendapat kebenaran dan kelulusan bertulis daripada pihak Unit Teknologi Maklumat.	**ICT dan bahagian masing- masing**

050304	Prosedur Kecemasan	Tindakan
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	**Semua dan Pegawai Keselamatan Jabatan**
0504	**Keselamatan Dokumen**	
Objektif: Melindungi aset ICT Pejabat Daerah dan Tanah Manjung dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
050401	**Dokumen**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	**Semua**

BIDANG 06

PENGURUSAN OPERASI DAN KOMUNIKASI

BIDANG 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

0601	**Pengurusan Perosedur Operasi**	
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.		
060101	**Pengendalian Prosedur**	**Tindakan**
	(a) Semua prosedur keselamatan ICT yang di wujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	**Semua**
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;	**Semua**

	(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 samaada sengaja atau pun tidak.	
060103	**Prosedur Pengurusan Insiden**	**Tindakan**
	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 PDTMJG, ICTSO**

0602	Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
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, ICTSO**
060202	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah mematuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**Pentadbir Sistem, ICTSO**

0603	**Perisian Berbahaya**	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan Trojan.		
060301	**Perlindungan dari Perisian Berbahaya**	**Tindakan**
	(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**

0604 Housekeeping		
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan Trojan.		
060401 Penduaan (Backup)		
	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**
060402 Sistem Log		**Tindakan**
	(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**

0605	**Pengurusan Rangkaian**	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060501	**Kawalan Infrastruktur Rangkaian**	
	Infrastruktur Rangkaian mestilah di kawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :- (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) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikongfigurasi oleh pentadbir sistem; (e) Semua Trafik keluar masuk hendaklah melalui firewall dibawah kawalan Pejabat Daerah dan Tanah Manjung; (f) 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"; (g) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pejabat Daerah dan Tanah Manjung hendaklah mendapat kebenaran ICTSO; dan (h) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	**BPM SUK PERAK / UICT**

0606	Pengurusan Media	
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.		
060601	**Penghantaran dan Pemindahan**	**Tindakan**
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	**Semua**
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 betul dan selamat.	**Semua**
060603	**Keselamatan Sistem Dokumentasi**	**Tindakan**
	(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**

0607	Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.		
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 Pejabat Daerah dan Tanah Manjung; (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 Bilangan1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan".	**Semua**

0608	**Pengerusan Mel Elektronik (e-mel)**	
	Penggunaan e-mel di SUK Perak hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang undang bertulis yang berkuatkuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh Pejabat Daerah dan Tanah Manjung 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 Pejabat Daerah dan Tanah Manjung; (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 sepuluh (10) 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;	**Semua**

	(i) E-mel yang tidak penting dan tidak menpunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (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".	

BIDANG 07

KAWALAN CAPAIAN

BIDANG 07 – KAWALAN CAPAIAN

0701	**Dasar Kawalan Capaian**	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT Pejabat Daerah dan Tanah Manjung.		
070101	**Keperluan Kawalan Capaian**	**Tindakan**
	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**
0702	**Pengurusan Capaian Pengguna**	
Objektif: Mengawal capaian pengguna ke atas aset ICT Pejabat Daerah dan Tanah Manjung.		
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;	**Pentadbir Sistem**

	(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) Bertukar bidang tugas kerja; (ii) Bertukar ke agensi lain; (iii) Bersara; atau (iv) Ditamatkan perkhidmatan.	
070202	**Jejak Audit**	**Tindakan**
	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 (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.	**Pentadbir Sistem ICT**

0703	Kawalan Capaian Sistem dan Aplikasi	
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
070301	**Sistem Maklumat dan Aplikasi**	
	Capaian sistem dan aplikasi di Pejabat Daerah dan Tanah Manjung adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian system 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.	

0704	**Peralatan Komputer Mudah Alih**	
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
070401	**Penggunaan Peralatan Komputer Mudah Alih**	**Tindakan**
	(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**

BIDANG 08

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

BIDANG 08 – PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801	**Keselamatan Dalam Membangunkan Sistem dan Aplikasi**	
Objektif: Memastikan sistem yang dibangunkan bersesuaian mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
080101	**Keperluan Keselamatan**	**Tindakan**
	(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**
0802	**Kawalan Kriptografi**	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
080201	**Penyulitan**	
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	**Semua**

080202	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	**Semua**
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**
0803	**Keselamatan Fail Sistem**	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
080301	**Kawalan Fail Sistem**	**Tindakan**
	(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 (d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistic, pemulihan dan keselamatan.	**Pentadbir Sistem ICT**

0804	**Pembangunan dan Proses Sokongan**	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401	**Prosedur Kawalan Perubahan**	
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai.	**Pentadbir Sistem ICT**

BIDANG 09

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BIDANG 09 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

0901	**Dasar Kesinambungan Perkhidmatan**	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
090101	**Pelan Kesinambungan Perkhidmatan**	**Tindakan**
	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) Mengenalpasti 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.	**ICTSO**

BIDANG 10

PEMATUHAN

BIDANG 10 – PEMATUHAN

1001	**Pematuhan dan Keperluan Perundangan**	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung.		
100101	**Pematuhan Dasar**	**Tindakan**
	Setiap pengguna di Pejabat Daerah dan Tanah Manjung hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Pejabat Daerah dan Tanah Manjung dan undang- undang atau peraturan – peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di Pejabat Daerah dan Tanah Manjung 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.	**Semua**
100102	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Pejabat Daerah dan Tanah Manjung: (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);	**Semua**

	(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.	

LAMPIRAN A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT

PEJABAT DAERAH DAN TANAH MANJUNG

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

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

.....

(Tandatangan)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO)

.....

( )

b.p. Pegawai Daerah
Pejabat Daerah dan Tanah Manjung
Perak Darul Ridzuan

Tarikh: .....

LAMPIRAN B

SURAT AKU JANJI KESELAMATAN SPTB

SURAT AKU JANJI KESELAMATAN SPTB

Saya.....No. Kad Pengenalan ..... dengan sesungguhnya berjanji dan berikrar untuk mematuhi peraturan di bawah sepanjang tempoh perkhidmatan saya di Unit ....., Pejabat Tanah Hulu Perak maka dengan itu saya berjanji, bahawa saya :

i. Tidak akan berkelakuan dengan cara yang boleh memburukkan atau mencemarkan nama Pejabat Pendaftar / Tanah;
ii. Melaksanakan tugas dengan cermat, bersungguh-sungguh, cekap, jujur, amanah dan bertanggungjawab;
iii. Tidak akan menggunakan kedudukan saya bagi mencari dan menggunakan maklumat dan aplikasi SPTB untuk faedah sesiapa jua pun tanpa kebenaran pemilik data;
iv. Akan menjaga kerahsiaan, kesahihan dan integriti maklumat serta data SPTB;
v. Bersetuju menukar katalaluan sistem setiap tiga (3) bulan;
vi. Tidak akan menulis, menampal, mempamer dan memberitahu kepada sesiapa dengan apa cara sekalipun, katalaluan sistem yang diberikan / yang telah ditukar;
vii. Tidak akan mencuba /memasuki mana-mana ruang SPTB yang tidak dibenarkan;
viii. Tidak akan mencuba mencatatkan / melumpuhkan SPTB melalui apa jua cara;
ix. Tidak akan memasang apa jua perisian ke dalam mana-mana komputer kepunyaan SPTB kecuali atas kebenaran pemilik data;
x. Tidak akan memasang atau menyambung apa jua peralatan yang tidak dibenarkan ke dalam rangkaian (*network*) SPTB;
xi. Akan mengimbas semua *portable* media untuk mengesan virus menggunakan perisian antivirus yang dibenarkan; dan
xii. Tidak akan menggunakan mana-mana perisian SPTB melainkan untuk urusan rasmi.

Saya menyedari bahawa mengingkari mana-mana peraturan diatas boleh menyebabkan saya dikenakan tindakan tartatertib atau diberhentikan serta merta tanpa syarat dan dikenakan tindakan undang
- undang.

Saya akan mematuhi janji-janji di atas walaupun saya tidak lagi berkhidmat di Pejabat Pendaftar / Tanah.

.....	.....
(Tandatangan)	**(Saksi)**
.....	.....
(Tarikh)	**(Cop Rasmi Jabatan)**