POLITEKNIK SULTAN HAJI AHMAD SHAH

DASAR KESELAMATAN ICT

VERSI 1.0 , MEI 2010

PENGENALAN

Dasar Keselamatan ICT POLISAS mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) POLISAS. Dasar ini juga menerangkan kepada semua pengguna ICT POLISAS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT jabatan. Dasar ini dibuat berasaskan kepada Dasar Keselamatan ICT MAMPU dan Dasar Keselamatan ICT Kementerian Pengajian Tinggi (KPT) yang sedia ada.

OBJEKTIF

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

SKOP

Dasar ini meliputi semua sumber atau aset ICT POLISAS yang digunakan seperti berikut :

a) **Data dan maklumat:** Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT;

b) **Peralatan ICT:** Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS), punca kuasa dan pendingin hawa;

c) **Media storan:** Semua media storan dan peralatan yang berkaitan seperti *thumb drives*, disket, kartrij, *CD-ROM*, pita, cakera, pemacu cakera dan pemacu pita;

d) **Peralatan komunikasi:** Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway, bridge, router* dan peralatan rangkain lain,

e) **Sistem teknologi:** Semua aplikasi yang mengendalikan, memproses, menyimpan dan menghantar data atau maklumat iaitu merangkumi sistem pangkalan data, protokol sistem rangkaian, topologi) dan aplikasi sistem lain. Ini termasuklah sistem pengoperasian, aturcara aplikasi, perisian utiliti, perisian komunikasi dan fail-fail data;

f) **Perisian ICT:** Semua perisian yang berkaitan dengan perkakasan peralatan ICT

g) **Dokumentasi:** Semua dokumen (prosedur dan manual pengguna) berkaitan

dengan pengoperasian dan pemasangan sistem dan aplikasi sama ada dalam bentuk elektronik atau bukan elektronik;

h) **Manusia:** Semua pengguna yang bertanggungjawab terhadap Keselamatan ICT POLISAS; dan

i) **Premis komputer dan komunikasi:** Semua kemudahan serta premis yang diguna untuk menempatkan semua aset yang disebutkan di atas.

Dasar ini adalah terpakai oleh semua pengguna di POLISAS termasuk kakitangan akademik, kakitangan bukan akademik, pembekal serta pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT POLISAS.

PRINSIP-PRINSIP

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

a. **Akses atas dasar perlu mengetahui**

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

b. **Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan 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 bertanggungjawab ke atas semua tindakannya terhadap aset ICT;

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 keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f. **Pematuhan**

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

g. **Pemulihan**

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

h. **Saling Bergantungan**

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

Perkara 1 : Pembangunan dan Penyelenggaraan Dasar

Dasar Keselamatan ICT	
1. Pelaksanaan Dasar	**Tindakan**
Pelaksanaan dasar ini akan dijalankan oleh Pengarah POLISAS selaku Ketua Pegawai Maklumat (CIO) dengan dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Pegawai Teknologi Maklumat selaku Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan serta Ketua Unit.	Pengarah
2. Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna ICT POLISAS (termasuk kakitangan, pembekal, pakar runding dan semua yang berkaitan).	ICTSO
3. Penyelenggaraan Dasar	
Dasar Keselamatan ICT POLISAS 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 POLISAS : a. Mengenalpasti dan menentukan perubahan yang diperlukan; b. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pengurusan atau JPICT; c. Perubahan yang telah dipersetujui oleh Jawatankuasa Pengurusan atau JPICT akan dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	ICTSO
4. Pemakaian Dasar	
Dasar Keselamatan ICT POLISAS adalah terpakai kepada semua pengguna ICT POLISAS dan tiada pengecualian diberikan.	Semua

Perkara 2 : Organisasi Keselamatan

Infrastruktur Organisasi Keselamatan	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
1. Ketua Pegawai Maklumat (CIO)	
Pengarah adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut : a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT POLISAS; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT POLISAS; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT POLISAS; e. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT POLISAS; f. Menentukan keperluan keselamatan ICT; g. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan h. Menentukan tindakan tatatertib yang perlu diambil ke atas pengguna yang telah dikenalpasti melanggar dasar Keselamatan ICT POLISAS.	Pengarah
2. Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) adalah merupakan Pegawai Teknologi Maklumat yang dilantik. Peranan dan tanggungjawab beliau adalah seperti berikut : a. Mengurus keseluruhan program-program keselamatan ICT	ICTSO

POLISAS; b. Menguatkuasakan Dasar Keselamatan ICT POLISAS; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT POLISAS kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT POLISAS; 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 Tindak balas Insiden Keselamatan ICT KPT (CERT KPT) atau GCERT MAMPU dan memaklumkannya kepada CIO; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. Menyiasat dan mengenalpasti pengguna yang melanggar Dasar Keselamatan ICT POLISAS; dan k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
3. Ketua Unit Pengurusan Sistem Maklumat (KUPSM)	
Peranan dan tanggungjawab KUPSM adalah seperti berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT POLISAS; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan POLISAS; c. Menentukan kawalan akses semua pengguna terhadap aset ICT POLISAS; d. Melaporkan penemuan mengenai pelanggaran Dasar Keselamatan ICT kepada ICTSO; dan	KUPSM

e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT di POLISAS.	
4. Pentadbir Sistem ICT	
Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat di Unit Pengurusan Sistem Maklumat yang dilantik adalah merupakan Pentadbir Sistem ICT POLISAS. 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 arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT POLISAS; c. Memantau aktiviti capaian harian pengguna; d. Mengenal pasti 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 mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	UPSM
5. Pengurus ICT Bahagian	
Semua Ketua Jabatan dan Ketua Unit adalah merupakan Pengurus ICT Bahagian. Peranan dan tanggungjawab Pengurus ICT Bahagian adalah seperti berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT POLISAS; b. Melaksanakan kawalan keselamatan ICT selaras dengan keperluan di setiap jabatan, unit dan bahagian; c. Menentukan kawalan akses semua pengguna terhadap aset ICT di setiap jabatan, unit dan bahagian;	Ketua Jabatan / Ketua Unit

d. Melaporkan penemuan mengenai pelanggaran Dasar Keselamatan ICT kepada KUPSM dan Pentabir Sistem ICT; e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT jabatan, unit dan bahagian.	
6. Pengguna	
Pengguna adalah merupakan semua kakitangan POLISAS. Peranan dan tanggungjawab pengguna adalah seperti berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT POLISAS; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat POLISAS; d. 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 diketahui umum; e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO, Pengurus ICT atau Pentadbir Sistem ICT dengan segera; f. Menghadiri program-program kesedaran mengenai keselamatan ICT; g. Bertanggungjawab ke atas aset-aset ICT di bawah jagaannya;dan	Semua Kakitangan POLISAS

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

Perkara 3 : Kawalan Aset dan Pengelasan Maklumat

Akauntabiliti Aset	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT POLISAS.	
1. Inventori Aset	
Semua aset ICT POLISAS hendaklah didaftar dan direkodkan. Ini termasuklah mengenal pasti, mengkategorikan aset dan merekodkan maklumat seperti pemilik, lokasi dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset Jabatan/Unit Semua
Pengelasan dan Penendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
1. 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	Semua
2. 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;	Semua

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, pengantaran, penyampaian, pertukaran dan pemusnahan; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

Perkara 4 : Keselamatan Sumber Manusia

Keselamatan ICT Dalam Tugas Harian	
Objektif : Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT jabatan.	
1. Tanggungjawab Keselamatan	
Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, di rekod, 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
2. Terma dan Syarat Perkhidmatan	
Semua warga POLISAS yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa.	Semua
3. Perakuan Akta Rahsia Rasmi	
Warga POLISAS yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
Menangani Insiden Keselamatan ICT	
Objektif : Meminimumkan kesan insiden keselamatan ICT.	
1. 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 mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail,	Semua

sistem kerap kali gagal dan kesilapan komunikasi; dan 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.	
Pendidikan	
Objektif : Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.	
1. Program Kesedaran Keselamatan ICT	
Setiap pengguna di POLISAS 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 POLISAS.	ICTSO
Tindakan Tatatertib	
Objektif : Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT POLISAS.	
1. Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT POLISAS akan dikenakan tindakan tatatertib.	Semua

Perkara 5 : Keselamatan Fizikal

Keselamatan Kawasan	
Objektif : Mencegah akses fizikal yang dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.	
1. Perimeter Keselamatan Fizikal	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a. Kawasan keselamatan fizikal hendaklah 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. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat; dan g. Mewujudkan perkhidmatan kawalan keselamatan.	Pengurus ICT Bahagian, CIO dan ICTSO
2. Kawalan Masuk Fizikal	
a. Setiap kakitangan POLISAS hendaklah memakai atau mengenakan kad ID Jabatan sepanjang waktu bertugas; b. Setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Pengawal Keselamatan; d. Hanya kakitangan dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu Jabatan.	Semua dan Pelawat

3. 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 POLISAS adalah bilik Pengarah, bilik-bilik Timbalan Pengarah, bilik server dan lain-lain kawasan yang diwartakan sebagai kawasan larangan. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal 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 penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Semua
Keselamatan Peralatan	
Objektif : Melindungi peralatan dan maklumat.	
1. 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 sempurna; 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	Semua

hendaklah dilaporkan kepada ICTSO.	
2. 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 sensitif diambil segera dari mesin pencetak.	Semua
3. Media Storan	
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan 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

4. Kabel	
Kabel komputer hendaklah dilindungi 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.	UPSM dan ICTSO
5. 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 UPSM atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; d. Semua penyelenggaraan mestilah mendapat kebenaran daripada KUPSM atau Pengurus ICT Bahagian berkenaan; dan e. Semua aktiviti penyelenggaraan perlu direkodkan.	Semua
6. 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 Ketua Jabatan/Ketua Unit dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;	Semua

c. Setiap jabatan dan unit bertanggungjawab untuk membuat pemeriksaan dari masa ke semasa bagi memastikan peralatan dipinjam digunakan dengan baik; d. Peminjam tidak dibenarkan membuat sebarang perubahan atau membaiki peralatan yang dipinjam atau memasukkan sebarang perisian tanpa kebenaran; e. Sekiranya peralatan hendak dipindahkan atau digunakan di tempat selain dari tempat yang dinyatakan, peminjam hendaklah memaklumkan kepada Ketua Jabatan dan Ketua Unit; dan f. Peminjam mestilah bertanggungjawab sepenuhnya ke atas peralatan sekiranya berlaku kerosakan ke atas peralatan tersebut. Sekiranya berlaku kerosakan, lapor segera kepada Juruteknik Komputer POLISAS.	
7. Peralatan di Luar Premis	
Bagi perkakasan yang dibawa keluar dari premis POLISAS, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan POLISAS : a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
8. 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 POLISAS : 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; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling	Semua

Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer".	
9. *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila warga tidak berada di tempatnya : a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
Keselamatan Persekitaran	
Objektif : Melindungi aset ICT POLISAS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
1. Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan POLISAS. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan 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;	Semua

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 ICT; 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.	
2. Bekalan Kuasa	
a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai; 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 berjadual.	PTM/ KUPSM
3. Prosedur Kecemasan	
a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan POLISAS yang dilantik.	Semua

Perkara 6 : Pengurusan Operasi dan Komunikasi

Pengurusan Prosedur Operasi	
Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
1. Pengendalian Prosedur	
a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti 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; c. Semua prosedur hendaklah dikemas kini dari semasa kesemasa atau mengikut keperluan; dan d. Semua kakitangan POLISAS hendaklah mematuhi prosedur yang telah ditetapkan.	Semua
2. Kawalan Perubahan	
a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada KUPSM terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen peralatan ICT hendaklah dikendalikan oleh Juruteknik Komputer atau pegawai yang diberi kuasa oleh CIO atau ICTSO; c. Semua aktiviti pengubahsuaian komponen peralatan ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat samaada secara sengaja atau pun tidak.	Semua
3. 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. Mengenalpasti 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.	ICTSO
Perancangan dan Penerimaan Sistem	
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
1. 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
2. Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi 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 seperti virus dan Trojan.	
1. 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 anti virus sebelum menggunakannya; d. Mengemaskini paten anti virus sekerap yang mungkin (sekurang-kurangnya sekali sehari); 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 baik pulih 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.	
1. 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 disimpan secara *off-site*. a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan 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
2. Sistem Log	
a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	UPSM
Pengurusan Rangkaian	
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
1. 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 di lokasi yang	UPSM

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 konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir system ICT; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan POLISAS; g. Semua perisian *sniffer* atau penganalisis rangkaian adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System* (IDS) atau *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat jabatan; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan POLISAS hendaklah mendapat kebenaran ICTSO; k. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; l. Sebarang penyambungan rangkaian daripada pihak ketiga (*remote tunneling*) ke dalam sistem rangkaian POLISAS hendaklah mendapat kebenaran ICTSO; m. Pengguna tidak dibenarkan mengubah kedudukan atau apa-apa maklumat yang terdapat di titik capaian rangkaian (*network access point*) ; n. Pengguna hendaklah menggunakan titik capaian rangkaian yang telah diberikan dan tidak boleh menukar kepada titik capaian yang	

lain; o. Sebarang perubahan atau kerosakan ke atas titik capaian rangkaian hendaklah dilaporkan kepada KUPSM atau ICTSO; dan p. Setiap penambahan atau penghapusan titik capaian rangkaian mestilah mendapat kelulusan KUPSM.	
Pengurusan Media	
Objektif : Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
1. Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pengarah terlebih dahulu.	Semua
2. 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 di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua

3. 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.	
1. Internet	
a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah 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 hak cipta terpelihara; e. Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan urusan rasmi kerajaan; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walaubagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Pengarah terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; g. Penggunaan internet adalah untuk tujuan penyelidikan, pengumpulan maklumat berfaedah dan pengendalian urusan rasmi sahaja. Penggunaan yang menjejaskan imej jabatan atau melayari laman web berunsur negatif adalah dilarang; h. Maklumat lanjut mengenai keselamatan internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003	Semua

bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	
2. Mel Elektronik	
a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh POLISAS sahaja boleh digunakan untuk tujuan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap akaun e-mel diberikan kapasiti sebanyak lapan puluh (80) Megabait bagi storan. c. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh POLISAS; d. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; e. Pengguna diminta berhati-hati sebelum membuka e-mel spam dan pastikan e-mel diterima daripada sumber yang benar; f. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; g. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; h. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; i. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; j. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; k. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; l. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; m. Penggunaan e-mel mestilah untuk tujuan yang dibenarkan sahaja.	Semua

Pengguna dilarang sama sekali menggunakan e-mel untuk tujuan yang menyalahi undang-undang seperti menyebar virus, maklumat palsu dan sebagainya; n. Pengguna adalah bertanggungjawab menyelenggara e-mel masing-masing seperti kerap membuat salinan (backup) emel. o. Pengguna tidak dibenarkan mendedahkan e-mel masing-masing kepada pihak yang tidak dkenali seperti mendaftarkan e-mel dalam laman web yang tidak dikenali; dan p. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	

Perkara 7 : Kawalan Capaian

Dasar Kawalan Capaian	
Objektif : Memahami dan mematuhi keperluan dalam mencapai dan menggunakan aset ICT jabatan.	
1. Keperluan Dasar	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	ICTSO

Pengurusan Capaian Pengguna	
Objektif : Mengawal capaian pengguna ke atas aset ICT jabatan.	
1. 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 diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; 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 akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) bulan, ii) bertukar bidang tugas kerja, iii) bertukar ke agensi lain, iv) tindakan keselamatan, v) bersara atau vi) ditamatkan perkhidmatan.	Semua

2. 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 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
Kawalan Capaian Sistem dan Aplikasi	
Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
1. Sistem Maklumat dan Aplikasi	
Capaian sistem dan aplikasi POLISAS adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi : a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir Sistem ICT, ICTSO

c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalah gunaan; 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. Walaubagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
Peralatan Komputer Mudah Alih	
Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.	
1. Penggunaan Peralatan Komputer Mudah Alih	
a. Merekodkan 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 yang selamat apabila tidak digunakan.	Semua

Perkara 8 : Pembangunan dan Penyelenggaraan Sistem

Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
1. 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 : i) sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, ii) sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul serta sempurna dan iii) sistem output untuk memastikan data yang telah diproses adalah tepat serta telus; c. Sebaiknya-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT, ICTSO
Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat.	
1. Pengurusan Kunci	
Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
1. Kawalan Fail Sistem	
a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang dibenarkan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan	Pentadbir Sistem ICT
Pembangunan dan Proses Sokongan	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
1. Kawalan Perubahan	
Perubahan atau pengubah suaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pentadbir Sistem ICT

Perkara 9 : Pengurusan Kesinambungan Perkhidmatan

Dasar Kesinambungan Perkhidmatan	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
1. Pelan Kesinambungan Perkhidmatan	
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 Jawatankuasa Pengurusan atau 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 mengemas kini pelan sekurang-kurangnya setahun sekali.	ICTSO

Perkara 10 : Pematuhan

Pematuhan dan Keperluan Perundangan
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT POLISAS.
1. Pematuhan Dasar

Setiap pengguna di POLISAS hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT POLISAS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di POLISAS termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Pengarah berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
2. Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di POLISAS : a. Arahan Keselamatan; b. Pekeliling Am Bil. 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 Bil. 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f. Surat Pekeliling Am Bil. 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender"; h. Surat Pekeliling Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan"; i. Akta Tandatangan Digital 1997; j. Akta Jenayah Komputer 1997; k. Akta Hak cipta (Pindaan) Tahun 1997; l. Akta Komunikasi dan Multimedia 1998; dan m. Akta Rahsia Rasmi 1972.	Semua