DASAR KESELAMATAN ICT

JABATAN AGAMA ISLAM NEGERI PERAK

PERAK DARUL RIDZUAN

Bahagian Teknologi Maklumat, Jabatan Agama Islam Negeri Perak
Tingkat 3, Kompleks Islam Darul Ridzuan
Jalan Panglima Bukit Gantang Wahab
30000 IPOH.
PERAK DARUL RIDZUAN

KANDUNGAN

PENDAHULUAN

Dasar Keselamatan ICT JAIPk adalah bagi menjamin segala urusan menyedia dan membekalkan perkhidmatan berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

4 komponen asas keselamatan ICT iaitu:-

i. melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
ii. menjamin setiap maklumat adalah tepat dan sempurna;
iii. mempastikan ketersediaan maklumat apabila diperlukan oleh pengguna;
iv. mempastikan akses kepada hanya pengguna-pengguna yang sah atau penerima maklumat .

Dasar Keselamatan ICT JAIPk ini juga bertujuan untuk menjamin keselamatan sumber maklumat dan kebolehsediaan kepada semua pengguna yang dibenarkan. Semua pengguna teknologi maklumat yang sah di JAIPk dibenarkan membuat capaian ke atas sistem yang bersesuaian. Capaian dikawal dan dipantau selaras dengan Dasar Keselamatan ICT JAIPk. Ciri-ciri utama keselamatan Sumber Maklumat Elektronik adalah seperti berikut:

- **Kerahsiaan**

  Sumber Maklumat Elektronik tidak boleh didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran pihak berkuasa.

- **Integriti**

  Data dan maklumat hendaklah tepat, lengkap dan dikemaskini. Ia hanya boleh diwujud, diubah atau dihapus oleh orang yang diberi

kuasa yang sah sahaja dan mengikut prosedur yang dibenarkan.

- **Tidak Boleh Disangkal**

  Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

- **Kesahihan**

  Data dan maklumat hendaklah dijamin kesahihannya.

- **Kebolehsediaan**

  Memastikan pengguna-pengguna yang sah boleh mencapai sumber maklumat. Menjalankan urusan pentadbiran awam bergantung kepada kebolehsediaan maklumat dan proses pengurusan.

1

PENGENALAN

1.1 Am

1.1.1 Definisi Dasar

Dasar Keselamatan ICT JAIPk ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset ICT JAIPk . Dasar ini juga menerangkan kepada semua pengguna di JAIPk mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JAIPk .

1.1.2 Objektif Dasar

Dasar Keselamatan ICT JAIPk diwujudkan untuk menjamin kesinambungan urusan JAIPk dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga adalah bagi menjamin keselamatan maklumat terperingkat dan maklumat rasmi kerajaan dari dicapai tanpa kuasa yang sah.

1.1.3 Skop Dasar

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

2

PRINSIP-PRINSIP

2.1 Prinsip-prinsip Asas

2.1.1 Akses atau Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atau 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.

2.1.2 Hak Akses Minimum

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

2.1.3 Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT JAIPk . Tanggungjawab ini perlu dinyatakan dengan jelas sesuai tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

2.1.4 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 yang bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail pengguna, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

2.1.5 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.*

2.1.6 Pematuhan

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

2.1.7 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.

2.1.8 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.

3

PENGURUSAN DAN TANGGUNGJAWAB DASAR KESELAMATAN ICT

3.1 Pelaksanaan Dasar

3.1.1 Pelaksanaan Dasar dan Ahli Jawatankuasa Keselamatan ICT

Pelaksanaan Dasar ini akan dijalankan dan dipengerusikan oleh Timbalan Pengarah Jabatan Agama Islam Perak merangkap CIO dibantu oleh Jawatankuasa Keselamatan ICT yang terdiri daripada pegawai-pegawai berikut:

i. Ketua Penolong Pengarah Bahagian Khidmat Pengurusan.
ii. Ketua Penolong Pengarah Bahagian Pembangunan Keluarga.
iii. Ketua Penolong Pengarah Bahagian Pendidikan.
iv. Ketua Penolong Pengarah Bahagian Penyelidikan.
v. Ketua Penolong Pengarah Bahagian Pendakwaan.
vi. Ketua Penolong Pengarah Bahagian Dakwah.
vii. Ketua Penolong Pengarah Bahagian Pengurusan Masjid.
viii. Ketua Penolong Pengarah Bahagian Penguatkuasaan Undang-undang Syariah.
ix. Pegawai Keselamatan ICT (ICTSO).
x. Pentadbir Sistem/Rangkaian/Pentadbir Web

3.2 Penyebaran Dasar

3.2.1 Dasar perlu disebarkan.

Dasar ini perlu disebarkan kepada semua pengguna JAIPk (termasuk kakitangan, pembekal, pakar runding dll.)

3.3 Penyelenggaraan Dasar

3.3.1 Semakan dan pindaan Dasar

Dasar Keselamatan ICT JAIPk 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 JAIPk :

i. kenalpasti dan tentukan perubahan yang diperlukan:
   - berdasarkan situasi ancaman.
   - berdasarkan situasi pencerobohan.
   - berdasarkan laporan maklumat insiden keselamatan.
   - berdasarkan cadangan yang diberi oleh pihak pengurusan.

ii. kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pengurusan ICT JAIPk ;

iii. perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan

iv. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun;

3.4 Pengecualian Dasar

3.4.1 Tiada siapa dikecualikan.

Dasar Keselamatan ICT JAIPk adalah terpakai kerana semua pengguna ICT JAIPk dan tiada pengecualian diberikan.

4

ORGANISASI KESELAMATAN ICT

4.1 Infrastuktur Keselamatan Organisasi

4.1.1 Tanggungjawab Ketua Pegawai Maklumat (CIO)

Timbalan Pengarah JAIPk adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab CIO adalah seperti berikut:

i. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JAIPk ;
ii. memastikan semua pengguna mematuhi Dasar Keselamatan ICT JAIPk . Tindakan sewajarnya hendaklah diambil apabila berlaku sebarang perlanggaran keselamatan;
iii. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi;
iv. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JAIPk dan
v. memastikan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan Dasar Keselamatan ICT JAIPk .

4.1.2 Tanggungjawab Ketua Penolong Pengarah Bahagian Khidmat Pengurusan (KPP BKP)

Peranan dan tanggungjawab Ketua Penolong Pengarah BKP JAIPk adalah seperti berikut:

i. membantu CIO JAIPk dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
ii. menentukan keperluan keselamatan ICT; dan

iii. membangun dan menyelaras perlaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.

4.1.3 Tangggungjawab ICTSO

Penolong Pegawai Teknologi Maklumat (PPTM) adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

i. mengurus keseluruhan program-program keselamatan ICT JAIPk ;
ii. menguatkuasakan Dasar Keselamatan ICT JAIPk ;
iii. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JAIPk kepada semua pengguna;
iv. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JAIPk ;
v. menjalankan pengurusan risiko;
vi. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
vii. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
viii. melaporkan insiden keselamatan ICT kepada pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO;
ix. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
x. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JAIPk dan
xi. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

4.1.4 Tanggungjawab Pentadbir Sistem

Penolong Pegawai Teknologi Maklumat (PPTM) atau mana-mana pegawai yang dilantik oleh jabatan untuk mentadbir sesuatu sistem ICT di JAIPk adalah merupakan Pentadbir Sistem ICT JAIPk . Peranan dan tanggungjawab adalah seperti berikut:

i. mengambil tindakan yang bersesuaian dengan segera ke atas aset ICT apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;
ii. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JAIPk ;
iii. memantau aktiviti capaian harian pengguna;
iv. mengenalpasti aktiviti-aktiviti tidak normal seperti pmncerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;
v. menyimpan dan menganalisis rekod jejak audit dan
vi. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.

4.1.5 Tanggungjawab Pegawai Pengkelasan Dokumen

Pegawai Pengkelasan Dokumen JAIPk ialah pegawai yang dilantik oleh Menteri Besar di bawah Akta Rahsia Rasmi 1972, perakuan di bawak Seksyen 2B yang dipertanggungjawab untuk mengelaskan apa-apa surat rasmi atau bahan sebagai "Rahsia Besar, Rahsia, Sulit atau Terhad".

4.1.6 Tanggungjawab Pengguna

Pengguna ialah semua kakitangan JAIPk , peserta kursus dan pihak kontraktor yang menjalankan kerja-kerja di JAIPk . Peranan dan tanggungjawab pengguna adalah seperti berikut:

i. membaca, memahami dan mematuhi Dasar Keselamatan ICT JAIPk ;
ii. mengetahui dan memahami implikasi keselamatan ICT, kesan dari tindakannya;
iii. lulus tapisan keselamatan;
iv. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat JAIPk ;
v. melaksanakan langkah-langkah perlindungan seperti:
    - menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    - memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
    - menentukan maklumat sedia untuk digunakan;
    - menjaga kerahsiaan kata laluan;
    - mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
    - memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
    - menjaga kerahsiaan langkah-langkah Keselamatan ICT dari diketahui umum.
vi. melaporkan sebarang aktiviti yang mengancam keselamatan ICT dengan segera;
vii. menghadiri program-program kesedaran mengenai keselamatan ICT; dan

viii. menandatangani surat akuan pematuhan Dasar Keselamatan ICT JAIPk .

5

KAWALAN DAN PENGELASAN ASET

5.1 Akauntabiliti Aset

5.1.1 Inventori Aset

Semua aset ICT JAIPK hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan dan Arahan Keselamatan hendaklah dipatuhi.

5.1.2 Pemilikan Aset

Setiap pengguna adalah bertanggungjawab ke atas semua aset di bawah kawalannya. Semua pengguna aset ICT JAIPK hendaklah mematuhi peraturan-peraturan penggunaan maklumat dan aset ICT yang telah ditetapkan oleh pihak pengurusan.

5.1.3 Pengelasan Maklumat

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut:

i. Rahsia Besar;
ii. Rahsia;
iii. Sulit; atau
iv. Terhad.

5.1.4 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan 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.

6

KESELAMATAN SUMBER MANUSIA

6.1 Keselamatan ICT Dalam Tugas Harian

6.1.1 Tanggungjawab Keselamatan

Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.

6.1.2 Terma dan Syarat Perkhidmatan

Semua warga JAIPK Perak yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa.

6.1.3 Perakuan Akta Rahsia Rasmi

Warga JAIPK Perak yang menguruskan maklumat terperingkat hendaklah mematuhi semua peraturan Arahan Keselamatan dan Akta Rahsia Rasmi 1972.

6.2 Menangani Insiden Keselamatan ICT

6.2.1 Pelaporan Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan dengan kadar segera:

i. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
ii. sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
iii. kata laluan atau mekanisme kawalan akses hilang, dicuri didedahkan atau disyaki hilang, dicuri atau didedahkan;
iv. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;
v. 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.

6.3 Pendidikan

6.3.1 Program Kesedaran Keselamatan ICT

Setiap pengguna di JAIPK Perak 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 JAIPK.

6.3.2 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT JAIPK akan dikenakan tindakan tatatertib.

7

KESELAMATAN FIZIKAL

7.1 Keselamatan Kawasan

7.1.1 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:

i. kawalan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
ii. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
iii. memperkukuhkan dinding dan siling;
iv. menghadkan jalan keluar masuk;
v. mengadakan kaunter kawalan;
vi. menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan
vii. mewujudkan perkhidmatan kawalan keselamatan.

7.1.2 Kawalan Masuk Fizikal

a. Setiap pengguna JAIPk hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di kaunter pengawal keselamatan aras G dan hendaklah dikembalikan semula selepas tamat lawatan;
c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan

apabila pengguna berhenti, bertukar atau bersara;

d. Setiap pelawat hendaklah mendaftar di kaunter pengawal keselamatan aras G.
e. Kehilangan pas keselamatan mestilah dilaporkan dengan segera;
f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JAIPk.

7.1.3 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 JAIPk adalah bilik Pengarah JAIPk, bilik Timbalan Pengarah JAIPk, bilik-bilik Ketua Penolong Pengarah JAIPk, bilik Pegawai-Pegawai Bahagian, bilik kebal dan bilik server. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja;

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.

7.1.4 Perkakasan

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:

i. setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;
ii. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai cirri-ciri keselamatan;
iii. setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan
iv. sebarang bentuk penyelewengan atau salah guna perkakasan

hendaklah dilaporkan kepada pegawai atasan.

7.1.5 Dokumen

Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

i. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
ii. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;
iii. menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. Penyulitan (*encryption*) bermaskud proses untuk mengubah data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses dekripsi (*decrypting*), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu; dan
iv. pada dasarnya, enkripsi (*encryption*) adalah proses untuk mengubah pesanan atau data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses dekripsi (*decrypting*), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu.
v. memastikan dokumen yang mengandungi bahan atau maklumat sulit diambil segera dari pencetak.

7.1.6 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 disimpan dalam media storan adalah terjamin dan selamat:

i. penyediaan ruang untuk penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
ii. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;
iii. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan
iv. pergerakan media storan hendaklah direkodkan.

7.1.7 Kabel

Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

i. menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
ii. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan
iii. melindungi laluan pemasangan kabel sepenuhnya.

7.1.8 Penyelenggaraan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.

i. semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan;
ii. perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; dan
iii. semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.

7.1.9 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:

i. peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan
ii. aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan dan mengikut prosedur yang ditetapkan oleh Bahagian Teknologi Maklumat (BTM).

7.1.10 Peralatan Di Luar Premis

Bagi perkakasan yang dibawa keluar dari premis JAIPk, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawasan JAIPk:

i. peralatan perlu dilindungi dan dikawal sepanjang masa; dan
ii. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

7.1.11 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 JAIPk:

i. semua kandungan peralatan ICT termasuk maklumat rahsia rasmi

hendaklah dihapuskan terlebih dahulu sebelum dilupuskan.

ii. sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan

iii. maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer" dan Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".

7.1.12 Clear Desk dan Clear Screen

Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian dan kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang rahsia terdedah sama ada atas meja atau di paparan skrin:

i. gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer;

ii. bahan-bahan rahsia hendaklah disimpan dalam laci atau cabinet fail yang berkunci.

7.2 Keselamatan Persekitaran

7.2.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil:

i. merancang dan menyediakan pelan keseluruhan susun atur data (bilik

percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;

ii. 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;

iii. peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;

iv. bahan mudah terbakar mestilah disimpan di luar kawasan kemudahan penyimpanan aset ICT;

v. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;

vi. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan

vii. semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

7.2.2 Bekalan Kuasa

Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

7.2.3 Prosedur Kecemasan

Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan.

Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.

8

PENGURUSAN KOMUNIKASI DAN OPERASI

8.1 Pengurusan Prosedur Operasi

8.1.1 Pengendalian Prosedur

Semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. 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. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.

8.1.2 Kawalan Perubahan

Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu.

Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.

Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak sengaja.

8.1.3 Kawalan Prosedur

Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan. Prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut:

i. mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
ii. menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
iii. menyimpan jejak audit dan memelihara bahan bukti; dan
iv. menyediakan tindakan pemulihan segera.

8.2 Perancangan dan Penerimaan Sistem

8.2.1 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 pasa 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.

8.2.2 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

8.3 Perisian Berbahaya

8.3.1 Perlindungan dan 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 *pattern anti virus*;
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.

8.4 Housekeeping

8.4.1 Penduaan

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang butirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site:*

i. membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

ii. membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan

iii. menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.

8.4.2 Sistem log

a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

b. Mewujudkan satu sistem log secara berpusat dan perlu dibuat pendua;

c. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

d. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan dengan segera kepada Pegawai Atasan.

8.5 Pengurusan Rangkaian

8.5.1 Kawalan Infrastuktur 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:

i. tanggungjawab atau kerja-kerja operasi rangkaian dan operasi komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

ii. peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

iii. capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

iv. semua peralatan mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi;

v. *firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi kerajaan serta dikonfigurasi oleh pentadbir sistem;

vi. semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JAIPk;

vii. semua perisian *sniffer* atau *network analyser* atau perisian seumpama dengannya adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

viii. memasang perisian *Instrusion Detection System (IDS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JAIPk;

ix. 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 Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";

x. sebarang penyambungan rangkaian yang bukan di bawah kawalan JAIPk hendaklah mendapat kebenaran ICTSO;

xi. semua pengguna hanya dibenarkan menggunakan rangkaian JAIPk sahaja. Penggunaan modem hendaklah mendapat kebenaran ICTSO;

xii. JAIPk berhak untuk menamatkan perkhidmatan rangkaian VPN (PerakNet) sesuatu jabatan atau agensi yang melalui *firewall* JAIPk sekiranya difikirkan tidak diperlukan lagi; dan

xiii. memastikan keperluan perlindungan ICT adalah bersesuaian dan

mencukupi bagi menyokong perkhidmatan yang lebih optimum.

8.5.2 Rangkaian Tanpa Wayar

Langkah-langkah minimum perlu dilaksanakan bagi memperkukuhkan kawalan keselamatan sistem rangkaian tanpa wayar. Berikut adalah langkah-langkah pengukuhan sistem rangkaian tanpa wayar:

i. langkah-langkah mesti mengikut Arahan Keselamatan dan para 4.4.3.3 Malaysian Public Sector Management of ICT Security Handbook (MyMIS) yang dikeluarkan oleh MAMPU pada 2001.

ii. melaksanakan inkripsi ke atas wireless access point (AP).

iii. meningkatkan keselamatan penggunaan wireless access point (AP) menerusi kaedah berikut:

- menggunakan enkripsi dan network key yang kukuh dengan kombinasi pelbagai character seperti alphabet, aksara khas dan nombor;
- kerap menukar kata laluan atau network key; dan
- kawalan penggunaan MAC Address.

iv. pengukuhan struktur rangkaian setempat boleh dilaksanakan seperti berikut:

- merekabentuk sistem rangkaian setempat supaya akses menerusi wireless access point (AP) perlu melalui tapisan keselamatan yang sewajarnya; dan
- merekabentuk kawalan capaian menggunakan pengenalan pengguna (user authentication) melalui penggunaan Radius Server.

v. pengukuhan keselamatan fizikal pula boleh dilaksanakan seperti berikut:

- memasang alat reflector yang akan mengawal pancaran signal radio wireless access point (AP) dalam jarak yang

dikehendaki

- menggunakan cat dinding khas yang dapat menghalang pancaran signal supaya dapat melampui jarak yang dikehendaki seperti *Defend Air Radio Shield Paint*; dan
- menggunakan *window shield* yang dapat menghalang signal daripada melepasi melalui tingkap.

8.6 Pengurusan Media

8.6.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pegawai Atasan terlebih dahulu.

8.6.2 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 dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.

8.6.3 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.

8.7 Keselamatan Komunikasi

8.7.1 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 yang dibenarkan oleh jabatan;

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 peraturan yang telah ditetapkan; dan

g. Maklumat lanjut mengenai keselamatan Interhet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".

8.7.2 Mel Elektronik (Emel)

a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh jabatan

sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh SUK Perak;

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 e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomukasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;

i. E-mel yang tidak penting dan tidak mempunyai nilai arkid 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 e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".

9

KAWALAN CAPAIAN

9.1 Dasar Kawalan Capaian

9.1.1 Keperluan Dasar

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

9.1.2 Akaun Pengguna

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

i. akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan;
ii. akaun pengguna mestilah unik;
iii. 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;
iv. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
v. pengguna akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
vi. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut;

- pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu;
- bertukar bidang tugas kerja;
- bertukar ke agensi lain;
- bersara; atau
- ditamatkan perkhidmatan

9.1.3 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:

i. maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;
ii. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
iii. 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.

9.1.4 Sistem Maklumat dan Aplikasi

Capaian sistem dan aplikasi di JAIPk adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-

langkah berikut hendaklah dipatuhi:

i. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;

ii. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;

iii. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;

iv. menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

v. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan

vi. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

9.2 Peralatan Komputer Mudah Alih

9.2.1 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.

10

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 Keselamatan Dalam Membangunakan Sistem dan Aplikasi

10.1.1 Keperluan Dasar

a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud 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.

10.2 Kriptografi

10.2.1 Penyulitan

Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

10.2.2 Tandatangan Digital

Pengguna tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.

10.2.3 Pengurusan Kunci (Key)

Pengurusan kunci (key) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci (key) berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

10.3 Sistem Fail

10.3.1 Kawalan Sistem Fail

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 statistik, pemulihan dan keselamatan.

10.4 Pembangunan dan Proses Sokongan

10.4.1 Kawalan Perubahan

Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.

11

KESINAMBUNGAN PERKHIDMATAN

11.1 Dasar Kesinambungan Perkhidmatan

11.1.1 Pelan Kesinambunagan Keselamatan

Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediakan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian:

i. mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

ii. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

iii. mendokumentasikan proses dan prosedur yang telah dipersetujui;

iv. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

v. membuat penduaan; dan

vi. menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

12

PEMATUHAN DASAR

12.1 Pematuhan dan Keperluan Perundangan

12.1.1 Pematuhan Dasar

Setiap pengguna di JAIPk hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JAIPk dan undang-undang atau peraturan-peraturan lain yang berkaitan dan masih berkuatkuasa.

Semua aset ICT di JAIPk termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

12.1.2 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JAIPk:

- Arahan Keselamatan;
- Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
- Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);

- Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

- Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";

- Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

- Akta Tandatangan Digital 1997;

- Akta Jenayah Komputer 1997;

- Akta Hak Cipta (Pindaan) Tahun 1997; dan

- Akta Komunikasi dan Multimedia 1998.
- Pekeliling-pekeliling dan prosedur-prosedur yang dikeluarkan dari masa ke semasa.

SINGKATAN

i.	**BTM**	-	Bahagian Teknologi Maklumat
ii.	**CIO**	-	Chief Information Officer
iii.	**GCERT**	-	Government Computer Emergency Response Team
iv.	**ICT**	-	Information Communication and Technology
v.	**ICTSO**	-	Information Security Officer
vi.	**JPICT**	-	Jawatankuasa Pengurusan Teknologi Maklumat
vii.	**KPP**	-	Ketua Penolong Pengarah
viii.	**KPKK**	-	Ketua Pegawai Keselamatan Kerajaan
ix.	**MAMPU**	-	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri
x.	**PKJ**	-	Pegawai Keselamatan Jabatan
xi.	**SUK Perak**	-	Pejabat Setiausaha Kerajaan Negeri Perak
xii.	**JAIPK**	-	Jabatan Agama Islam Negeri Perak
xiii.	**AP**	-	Access Point
xiv.	**UPS**	-	Uninterruptable Power Supply
xv.	**Kriptografi**	-	Tersembunyi, Rahsia