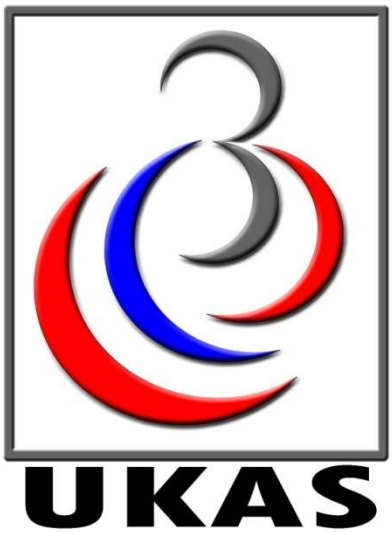

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

Unit Kerjasama Awam Swasta

ISI KANDUNGAN

DASAR KESELAMATAN

TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

1.0 PENGENALAN

1.1 Pendahuluan

Untuk memodenkan perkhidmatan sejajar dengan matlamat kerajaan semua urusan harian Unit Kerjasama Awam Swasta (UKAS) telah dilaksanakan secara elektronik dengan menggunakan kemudahan ICT. Namun begitu penggunaan kemudahan ICT ini terdedah kepada penyalahgunaan yang akan menyebabkan maklumat dibocorkan, diubah atau dirosakkan sama ada secara kebetulan atau dengan sengaja. Oleh yang demikian adalah perlu bagi UKAS menyediakan satu dasar keselamatan ICT yang dapat melindungi semua kepentingan ICT dari ancaman-ancaman yang tidak diingini.

1.2 Tujuan dan Skop

Dasar keselamatan ini bertujuan memberi panduan tentang langkah-langkah yang perlu dipatuhi untuk memastikan keselamatan ICT terjamin. Ia merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasuk, diwujud, dimusnah, disimpan ,dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan ke dalam semua aset ICT. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosidur dalam pengendalian semua perkara-perkara berikut:-

i. Data dan maklumat – Semua data dan maklumat yang disimpan atau digunakan dipelbagai media atau peralatan ICT.

ii. Aset ICT – Semua peralatan komputer dan periferal seperti komputer peribadi, worksation, server dan alat-alat prasarana seperti Uninterrupted Power Supply (UPS), punca kuasa dan penghawa dingin.

iii. Media storan – Semua media storan dan peralatan yang berkaitan seperti disket, katrij, CDROM, pita ,cakera, pemacu cakera, pemacu pita dan pen drive.

iv. Komunikasi dan peralatan rangkaian – Komunikasi seperti server rangkaian, gateway, bridge, router, switch dan peralatan PABX.

v. Perisian – Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan menghantar maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data.

vi. Dokumentasi – Semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, transparencies , risalah dan slides.

vii. Manusia – Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggung jawab terhadap keselamatan ICT.

viii. Premis Komputer – Semua kemudahan serta premis yang diguna untuk menempatkan perkara (i) hingga (vii) diatas.

Dasar ini terpakai di semua pejabat UKAS dan tempat-tempat yang mempunyai aset ICT UKAS di seluruh negara.

2.0 OBJEKTIF DAN PRINSIP POLISI KESELAMATAN ICT UKAS

2.1 Objektif

Objektif utama polisi keselamatan ICT UKAS adalah untuk :-

i. Memastikan kelancaran operasi jabatan dan meminimumkan kerosakan atau kemusnahan.

ii. Melindungi kepentingan pihak-pihak yang bergantung pada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

iii. Mencegah salahguna atau kecurian aset ICT jabatan.

2.2 Prinsip

Prinsip-prinsip yang menjadi asas polisi keselamatan ICT UKAS adalah:-

2.2.1 Akses Atas Dasar Perlu Mengetahui (a need to know basis)

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 akses di bawah prinsip ini adalah berasaskan klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut:-

i. Klasifikasi maklumat

Keselamatan ICT jabatan hendaklah mematuhi ”Arahan Keselamatan” Perenggan 53, mukasurat 15, dimana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi daripada pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dihantar secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad.

ii. Tapisan Keselamatan Pengguna

Dasar keselamatan ICT Jabatan adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latarbelakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

2.2.2 Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan,mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

2.2.3 Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa.

iii. Menentukan maklumat sedia untuk digunakan.

iv. Menjaga kerahsiaan katataluan.

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, pertukaran dan pemusnahan.

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

2.2.4 Pengasingan

Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data dilakukan secara berasingan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, dimanipulasi dan seterusnya mengekalkan integriti dan kebolehsediaan.

Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:-

i. Persekitaran pembangunan dimana sesuatu dalam proses pembangunan.

ii. Persekitaran penerimaan iaitu peringkat dimana sesuatu aplikasi diuji.

iii. Persekitaran sebenar dimana aplikasi sedia untuk dioperasikan.

2.2.5 Pengauditan

Pengauditan ialah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti 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 dan audit trail. Audit trail penting apabila wujud keperluan untuk mengenalpasti punca masalah atau ancaman kepada keselamatan ICT. Rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta.

Pengauditan juga perlu dibuat pada rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong audit trail sistem komputer.

Sistem pengauditan penting dalam menjamin akauntabiliti. Antara lain sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:-

i. Mengesan pematuhan atau pelanggaran keselamatan.

ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya pelanggaran keselamatan.

iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya pelanggaran keselamatan.

2.2.6 Pematuhan

Pematuhan merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran polisi. Pematuhan kepada polisi keselamatan ICT jabatan boleh dicapai melalui tindakan berikut:-

i. Mewujud proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan.

ii. Merumus pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenalpasti.

iii. Melaksana program pemantuan keselamatan secara beterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi.

iv. Menguatkuasa amalan melapor sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

2.2.7 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:-

i. Merumus dan menguji Pelan Pemulihan Bencana (Disaster Recovery Plan). UKAS akan merancang pelan pemulihan bencana selepas pelaksanaan sistem pengurusan pengauditan.

ii. Mengamalkan langkah-langkah salinan data dan lain-lain amalan baik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan clean desk.

2.2.8 Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap-melengkapi antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat dimana ditahap minimum, mengandungi langkah-langkah berikut:-

i. **Sambungan kepada Internet** – semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisma pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui gateway firewall yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu penggunaan modem dalaman tidak dibenarkan.

ii. **Backbone rangkaian** – Backbone rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan.

iii. **Rangkaian jabatan** – Semua rangkaian jabatan akan dihubungkan ke backbone melalui firewall yang akan mengkod semua trafik di antara rangkaian di peringkat yang seterusnya atau pusat data.

iv. **Server jabatan** – Hanya data dan maklumat yang kritikal atau sensitif sahaja yang akan disimpan di server jabatan yang diurus secara berpusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

3 INFRASTRUKTUR/ORGANISASI KESELAMATAN

3.2 Jawatankuasa Pemandu Keselamatan ICT

i Keanggotaan

a Ketua Pengarah (KP)

b. Timbalan Ketua Pengarah (Pembangunan) sebagai Chief Information Officer (CIO).

c. Ketua Pengarah (Dasar) sebagai Pegawai Keselamatan Jabatan (PKJ)

d. Pegawai Teknologi Maklumat Kanan Unit Teknologi Maklumat dan Komunikasi (ICT) sebagai Pengurus ICT.

e. Pegawai Teknologi Maklumat sebagai Pegawai Keselamatan ICT

(ICTSO).

ii Urusetia

a. Unit Teknologi Maklumat dan Komunikasi (ICT)

iii Bidang Tugas

a. Menggariskan Dasar Keselamatan bagi UKAS selaras dengan kuasa

undang-undang yang dipertanggungjawabkan.

b. Menentukan langkah keselamatan dari segi teknikal, fizikal dan

pentadbiran yang patut digunakan bagi melindungi maklumat-maklumat

yang direkodkan di dalam semua sistem di UKAS.

c. Membuat keputusan dan menentukan tahap capaian maklumat terhadap

semua permohonan capaian kepada semua sistem di UKAS.

d. Menentukan langkah-langkah yang patut di ambil bagi agensi-agensi luar

yang melanggar perjanjian ke atas penggunaan maklumat yang

menjejaskan keselamatan sistem-sistem di UKAS.

e. Membuat ketentuan bagi sebarang kes kesangsian terhadap keselamatan sistem-sistem di UKAS

3.2 Ketua Pengarah (KP)

Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut:

i. Memastikan semua pengguna memahami peruntukan di bawah Dasar Keselamatan ICT UKAS.

ii. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT UKAS.

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 UKAS.

3.2 Chief Information Officer (CIO)

CIO bertanggungjawab melaksanakan perkara-perkara berikut:-

i. Bertanggungjawab kepada KP dalam melaksanakan dasar keselamatan Jabatan.

ii. Merangka pelan tindakan keselamatan ICT Jabatan.

iii. Memastikan pelaksanaan dasar keselamatan ICT.

3.3 Pengurus ICT

Penolong Pengarah Kanan Unit Teknologi Maklumat dan Komunikasi (ICT) adalah merupakan Pengurus ICT UKAS. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

i. Membaca, memahami dan mematuhi Dasar Keselamatan ICT UKAS.

ii. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan UKAS.

iii. Menentukan kawalan akses semua pengguna terhadap aset ICT UKAS.

iv. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO.

v. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT UKAS.

3.4 Pegawai Keselamatan Jabatan

Pegawai Keselamatan Jabatan bertanggungjawab dalam pentadbiran keselamatan Jabatan secara keseluruhannya. Fungsi dan tanggungjawab beliau merangkumi aspek-aspek berikut:-

i. Memelihara hubungan (liaison) dengan Ketua Pegawai Kerajaan, Pegawai Keselamatan Kerajaan Negeri, Ketua Polis Negeri/Daerah dan Ketua Bomba Negeri/Daerah.

ii. Menasihati Ketua Jabatan mengenai langkah-langkah keselamatan perlindungan jabatan (sejajar dengan perubahan keadaan) mencakupi keselamatan fizikal, dokumen dan personel dengan berpandukan Buku Arahan Keselamatan).

iii. Mengeluarkan arahan tetap keselamatan untuk semua pegawai-pegawai / kakitangan-kakitangan supaya mereka benar-benar sedar tentang tanggungjawab mereka terhadap keselamatan tempat mereka bekerja.

iv. Mengatur rancangan pendidikan keselamatan agar semua pegawai/kakitangan tahu sebab-sebab arahan-arahan/peraturan-peraturan keselamatan wajib dipatuhi untuk berhadapan dengan ancaman espionaj, sabotaj dan subversive.

v. Sentiasa menguji dan mengulang kaji ketahanan kaedah keselamatan yang sedang digunakan berasaskan penilaian ancaman keselamatan semasa melalui pemeriksaan mengejut.

vi. Menyediakan langkah-langkah keselamatan perlindungan bangunan-bangunan rasmi bagi mengecilkan angkara kekerasan, pengkhianatan termasuk ancaman bom palsu.

vii. Menyiasat semua perbuatan pelanggaran keselamatan dan menyediakan laporan mengandungi rumusan dan perakuan kepada Ketua Jabatan.

viii. Mengarah Pendaftar Rahsia / Sulit menyelenggara rekod semua pelanggaran keselamatan yang dilakukan semua pegawai/kakitangan.

ix. Memastikan alat-alat mencegah kebakaran sentiasa dalam keadaan baik.

x. Memastikan semua kakitangan, pengguna, kontraktor, pembekal dan pelawat mematuhi Dasar keselamatan ICT UKAS dan garispanduan seperti yang termaktub di Buku Arahan Keselamatan dan Surat Pekeliling Am.

xi. Melaporkan semua insiden keselamatan ICT yang berlaku di Jabatan kepada KP dan Ketua Pegawai Keselamatan Jabatan/CIO, MAMPU mengikut Pekeliling Am Bil /2001-Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)

3.5 Pegawai Keselamatan ICT (ICTSO)

Pegawai keselamatan ICT bertanggungjawab untuk membangun, melaksana dan menyelenggara program-program Keselamatan ICT Jabatan. Peranan dan tanggungjawab Pegawai Keselamatan ICT termasuk:-

i. Mengurus keseluruhan program Keselamatan ICT Jabatan.

ii. Menguatkuasa dasar, standard dan garis panduan Keselamatan ICT jabatan

(dokumen ini hendaklah sentiasa dikemaskini selaras dengan perubahan teknologi, hala tuju organisasi dan ancaman).

iii. Membantu dalam membangunkan piawai atau garis panduan yang khusus selaras dengan keperluan dasar keselamatan ICT untuk suatu aplikasi spesifik dalam jabatan.

iv. Mengkaji sistem-sistem ICT bagi mengenalpasti kelemahan risiko dan vulnerability terhadap keperluan keselamatan.

v. Melaksanakan audit bagi mengenalpasti pelanggaran dasar, standard atau garis panduan keselamatan ICT yang telah ditetapkan (non compliance).

vi. Memastikan setiap keperluan pengecualian dasar hendaklah selaras dengan analisis penerimaan risiko.

vii. Mencadangkan penyelesaian bagi mengatasi sebarang pelanggaran dasar (non compliance).

viii. Mengkaji dan meneliti laporan-laporan audit berkaitan keselamatan ICT.

ix. Mengesahkan bahawa ancaman-ancaman utama kepada aset-aset maklumat telah dikenalpasti dan difahami oleh pihak pengurusan.

x. Sentiasa mengemaskini maklumat tentang ancaman-ancaman terbaru, teknologi pemprosesan dan juga kawalan dan kaedah perlindungan maklumat yang terbaru.

xi. Menyedia dan menyebar amaran berkenaan ancaman yang serius dan ketara terhadap asset-aset maklumat, seperti serangan virus komputer.

xii. Menubuhkan sebuah pasukan bertindak keselamatan untuk menangani insiden keselamatan ICT.

xiii. Menyelaras atau membantu dalam siasatan ancaman atau serangan ke atas aset maklumat.

xiv. Membantu dalam aktiviti pemulihan selepas serangan.

xv. Membuat laporan berkenaan isu keselamatan ICT kepada Pengurus Komputer, Pegawai Keselamatan Jabatan dan CIO.

xvi. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU.

4.0 STRATEGI PENGURUSAN DAN KESELAMATAN ICT / ANALISA RISIKO

UKAS perlu membuat analisa risiko ancaman keselamatan ICT setahun sekali. Ini untuk memastikan operasi Jabatan berterusan dengan meminimumkan kerosakan dan mengelakkan insiden-insiden keselamatan. Pihak pengurusan perlu mengambil langkah untuk mengurangkan risiko, menerima dan memantau baki risiko.

4.1 Risiko-Risiko Dan Sensitiviti Maklumat

Mengenalpasti risiko dan ancaman adalah langkah yang kritikal untuk melindungi aset ICT. Ini akan dapat menyelamatkan Jabatan dari mendapat malu disebabkan oleh pendedahan maklumat yang tidak sepatutnya. Setelah dapat mengenalpasti risiko-risiko dan ancaman tersebut satu langkah yang teratur perlu di ambil untuk menangani risiko dan ancaman tersebut. Aktiviti ini sepatutnya dapat mengelakkan urusniaga jabatan daripada ditutup atau sekurang-kurangnya mengurangkan gangguan.

Untuk mengenalpasti risiko dan ancaman, ICTSO, CIO dan semua pentadbir perlu melakukan langkah-langkah berikut:-

i. Menilai semula maklumat yang terkandung dalam sistem. Setelah ini dilakukan, nilai yang dikaitkan dengan aset ICT boleh mengenalpasti tahap dan jenis risiko yang boleh ditoleransi.
ii. Mengenalpasti peristiwa yang akan menyebabkan gangguan operasi harian.
iii. Menetapkan keutamaan kepada elemen risiko yang dikenalpasiti

4.2 Pengenalan Maklumat Organisasi

4.2.1 Klasifikasi maklumat

Maklumat rasmi boleh dikategorikan kepada:-

i. Rahsia Besar

ii. Rahsia, Sulit dan Terhad sepertimana yang termaktub di dalam Arahan Keselamatan.

Kandungan maklumat yang telah diwujudkan secara digital juga mengikut klasifikasi yang sama. Walau bagaimanapun, perlindungan kepada maklumat digital perlu dilakukan dengan cara yang sesuai seperti encryption, pengkodan warna dan melabel.

4.3 Jenis Ancaman

Diantara ancaman-ancaman yang dikenalpasti ialah:-

4.3.1 Ralat dan kesilapan memasukkan data

Kesilapan sering terjadi dalam operasi harian semasa memproses data atau maklumat oleh pengguna. Kesilapan yang sedemikian kemungkinan disebabkan salah memasukkan data atau kesilapan pemprograman dan ini merupakan ancaman kepada intergriti data dan keseluruhan sistem. Contohnya ialah penipuan dalam kemasukan data, kebocoran data dan sebagainya.

4.3.2 Penipuan, rompakan dan penyamaran

Maklumat yang dicuri atau digunakan untuk tujuan penipuan. Salahlaku jenayah ini boleh dilakukan oleh individu atau kumpulan, orang dalaman atau luar atau bekas kakitangan yang masih mendapat capaian ke sistem komputer. Contohnya termasuk pencuri maklumat dan penceroboh.

4.3.3 Sabotaj oleh pekerja

Pelakuan pekerja untuk memusnahkan sistem yang sedia ada seperti:-

- Memusnahkan perkakasan atau kemudahan untuk memastikan sistem ICT tidak dapat digunakan seperti kerosakan rangkaian, kehilangan peralatan perkakasan yang mengakibatkan tidak dapat digunakan.
- Memusnahkan program atau data untuk memutuskan perjalanan operasi sistem ICT.
- Memasukkan data yang salah yang mengakibatkan hasil yang dikeluarkan salah.
- Menghapuskan data untuk memastikan data tidak ada semasa pengeluaran dan
- Memasang pepijat program seperti virus ke dalam sistem ICT.
- Membuang akaun sistem bekas pekerja kerana berpindah, berhenti bekerja atau berpencen dengan serta-merta.

4.3.4 Hilang sokongan fizikal dan infrastruktur

Kehilangan yang disebabkan oleh gangguan elektrik, kehilangan komunikasi data, kebocoran air, kebakaran, banjir, ancaman bom dan rusuhan atau mogok yang akan mengganggu operasi perkhidmatan.

5.0 KESELAMATAN PERISIAN DAN PERKAKASAN

5.1 Pengenalpastian dan Pengesahan

Semua pengguna yang menggunakan perkakasan dan perisian dikenali melalui ID pengguna dan katalaluan. ID Pengguna adalah unik dan katalaluan adalah rahsia. Pengurusan penggunaan ID dikawal selia oleh pentadbir sistem. ID Pengguna dan katalaluan digunakan untuk mengawal pelaksanaan. Ia merupakan satu langkah keselamatan yang digunakan untuk menghadkan penggunaan server kepada pihak yang dibenarkan sahaja.

5.2 Kawalan Capaian

i. Penggunaan perisian hanya kepada orang tertentu sahaja. Pihak yang mengawal penggunaan ID hendaklah memastikan tiada ID yang diwujudkan tanpa mendapat kelulusan dan Fail Log hendaklah diselenggara oleh Pentadbir Sistem untuk tujuan pengauditan. ID tidak boleh dipinjamkan kepada orang lain untuk apa jua urusan. Bagi memastikan ia tidak disalahgunakan Pentadbir Sistem akan memantau dengan menyenak senarai ID dari semasa ke semasa.

ii. Dua salinan Senarai Kawalan Pengguna hendaklah dikeluarkan oleh Pentadbir Sistem. Salinan pertama disimpan oleh Pentadbir Sistem sementara salinan kedua diserahkan kepada bahagian yang berkenaan.

iii. Sebarang percubaan logon yang tidak sah perlu disiasat oleh Pentadbir Sistem dan melaporkan kejadian tersebut kepada ICTSO.

iv. Permintaan baru untuk menggunakan sistem perkhidmatan maklumat mestilah mendapat kelulusan keselamatan daripada Jawatankuasa Pemandu Keselamatan Jabatan. PTM (Aplikasi) mestilah memastikan ke semua ciri-ciri keselamatan kepada hal-hal yang berkaitan dijelaskan dalam arahan dan syarat-syarat penggunaan maklumat kepada bahagian operasi yang berkenaan seperti:-

a. Spesifikasi yang tepat mengenai kriteria untuk capaian maklumat.
b. Spesifikasi yang tepat mengenai penggunaan hasil ke penggunaan hasil keluaran (output)
c. Spesifikasi yang tepat mengenai permintaan untuk mendapatkan kebenaran untuk menggunakan hasil keluaran (output)
d. Permintaan perlu diberi satu siri nombor tugas.

v. Pentadbir Sistem perlu mengawal kerja-kerja yang akan dijalankan pada setiap hari

5.3 Accounting dan Audit Trail

i ICTSO yang dilantik perlu mengadakan lawatan mengejut sekurang-kurangnya setahun sekali ke semua unit-unit atau bahagian-bahagian yang sistem keselamatannya tertakluk dibawah pengawasannya.

ii ICTSO perlulah melaporkan aktiviti yang dijalankan kepada CIO. Laporan tersebut dibahagikan kepada laporan-laporan status bulanan dan laporan-laporan khas.

5.4 Full Deletion

Semua pengguna diperlukan melakukan backup ke atas data, aplikasi atau perisian yang terpaksa menjalani full deletion semasa pemasangannya. Data, aplikasi dan perisian ini perlu melalui ujian sepenuhnya bagi memastikan pemasangan semula adalah betul.

5.5 Perisian Merbahaya (Malicious Software)

Semua perisian merbahaya tidak dibenarkan dipasang pada server, workstation dan PC Jabatan. Pentadbir komputer Unit ICT mempunyai hak mutlak untuk memasuki sistem komputer pengguna tanpa perlu meminta kebenaran dari pengguna bagi memantau sebarang akitiviti dan instalasi perisian yang dilakukan oleh pengguna komputer UKAS.

5.7 Keselamatan Komputer

i. Setiap perkakasan komputer perlu dilabel dengan nombor inventori bagi memudahkan pengenalpastian perkakasan tersebut apabila berlaku kehilangan atau kecurian. Senarai inventori perkakasan tersebut hendaklah disimpan di Bahagian Kewangan dan Unit Sokongan Teknikal ICT. Ini bagi membantu proses pengauditan.

ii. Setiap pengguna komputer digalakkan mengguna ID dan katalaluan yang unik bagi mengelak penyalahgunaan perkakasan tersebut.

iii. Setiap pengguna perlu memastikan semua perkakasan dimatikan sebelum keluar dari pejabat.

iv. Pengguna perlu meminta kebenaran dari Unit ICT apabila perkakasannya perlu ditingkatkan (upgrade)

v. Semua perisian di UKAS dikawalselia oleh Unit ICT. Sekiranya pengguna ingin meminjam perisian tersebut perlu mengisi buku daftar perisian.

vi. Semua perisian cetak rompak tidak dibenarkan sama sekali dipasang pada perkakasan tersebut.

vii. Setiap peminjaman perisian mesti dipulangkan kembali kepada Sub-Unit Teknikal, Unit ICT.

5.7 Keselamatan Notebook

i. Unit-unit notebook yang ada di UKAS digunasama oleh pegawai dan kakitangan yang memerlukannya. Unit-unit ini dikawalselia oleh Unit ICT.

.

ii. Setiap perkakasan komputer perlu dilabel dengan nombor inventori bagi

memudahkan pengenalpastian perkakasan tersebut apabila berlaku kehilangan atau kecurian. Senarai inventori perkakasan tersebut hendaklah disimpan di Bahagian Kewangan dan Unit ICT. Ini membantu proses pengauditan.

iii. Setiap pengguna komputer dimestikan mengguna ID dan katalaluan yang unik bagi mengelak penyalahgunaan perkakasan tersebut.

iv. Setiap pengguna perlu memastikan semua perkakasan dimatikan sebelum keluar dari pejabat.

v. Pengguna perlu meminta kebenaran dari Unit ICT Sektor dan Negeri apabila perkakasannya perlu ditingkatkan (upgrade).

vi. Pengguna perlu mengisi buku log yang disediakan sebelum membuat pinjaman notebook.

vii. Notebook disimpan di tempat selamat dan berkunci bagi mengelakkan kecurian.

viii. Setiap peminjaman perkakasan dan perisian mesti dipulangkan kembali kepada Unit Sokongan Teknikal ICT.

6.0 KAWALAN KESELAMATAN KOMUNIKASI

6.1 Pengenalan

Beberapa langkah dan kaedah keselamatan digunakan bagi memastikan rangkaian komputer, data, aplikasi serta hos selamat untuk digunakan. Perkakasan dan perisian tertentu telah dipasang pada workstation dan pelayan untuk memastikan sistem komputer UKAS tidak dicerobohi.

Sistem rangkaian (WAN dan LAN) merangkumi keseluruhan perhubungan (connection) antara Ibu Pejabat dengan Cawangan Negeri. Keselamatan sistem rangkaian komputer terletak di bawah tanggungjawab Unit Rangkaian dan Pangkalan Data di Unit ICT. Ia ditadbir oleh kakitangan dari unit tersebut.

6.2 Infrastruktur Rangkaian

i. Router

Pemeriksaan setiap seminggu sekali dilakukan oleh pentadbir sistem memastikan router berfungsi dengan baik.

ii. Kawalan talian di cawangan

Pentadbir rangkaian mengawasi rangkaian setiap hari untuk memastikan semua talian berkeadaan baik. Sekiranya berlaku sebarang masalah pada talian rangkaian, pentadbir sistem akan melaporkan kepada helpdesk MAMPU.

6.3 Internet

6.3.1 Penggunaan Internet

Penggunaan internet di UKAS hanya diperuntukkan untuk urusan rasmi sahaja. Pentadbir sistem mengawal penggunaan sistem komputer atau rangkaian bagi memastikan ia selamat daripada dicerobohi. Pada masa ini semua pengguna yang mempunyai tugasan rasmi yang perlu dilakukan melalui internet boleh menggunakan kemudahan internet. Contohnya pegawai yang terlibat dengan aplikasi kerajaan elektronik seperti e-PEROLEHAN / e-SPKB dan juga e-mel rasmi jabatan.

Sesetengah protokol telah disekat dan jika pengguna memerlukan sesetengah protokol yang tidak dibenarkan bagi tujuan tugas rasmi, pengguna perlu meminta kebenaran Pengurus ICT serta kelulusan Pengarah masing-masing.

6.3.2 Perisian Firewall

i. Firewall digunakan untuk menilai setiap paket data di antara komputer dan internet dan buat keputusan bedasarkan arahan yang telah diberikan samada untuk halang, biar atau lepas (permit, block, ignore). Sesetengah firewall juga menyimpan log bagi membolehkan pihak pentadbir melihat dan menyelia apa yang telah berlaku.

ii. Pentadbir firewall perlu dilantik oleh pihak pengurusan keselamatan. Pentadbir firewall bertanggungjawab untuk mengawalselia firewall.

iii. Pentadbir firewall perlu mengenalpasti setiap versi perisian firewall yang terkini dan ditingkatkan jika perlu.

iv. Semua patch keselamatan yang disyorkan oleh pihak pembekal perlu dilaksanakan jika perlu.

v. Pentadbir firewall perlu memberi nombor telefon pejabat, telefon rumah dan telefon bimbit bagi membolehkan mereka dihubungi jika perkhidmatan mereka diperlukan.

6.3.3 Antivirus

i. Perisian Antivirus perlu dipasang pada semua Server komputer peribadi dan notebook bagi mengenalpasti dan mengimbas virus yang wujud di dalam server tersebut.

ii. Perisian perlu dibuat live update seminggu sekali sebelum membuat pengimbasan.

iii Pentadbir sistem perlu mengenalpati perisian antivirus yang terkini dan ditingkatkan jika perlu.

iv Penggunaan antivirus selain daripada yang digunapakai oleh UKAS perlu mendapat kebenaran dari Unit ICT.

6.3.4 Perkakasan

Setiap perkakasan dilabelkan nombor inventori bagi membolehkan ia dikenalpasti dengan mudah apabila berlaku kehilangan atau kecurian.

7.0 KAWALAN KESELAMATAN FIZIKAL ICT UKAS

7.1 Pengenalan

Keselamatan fizikal bermaksud memastikan bangunan, premis atau tempat termasuk yang digunakan bagi mengurus perkara-perkara terperingkat dan sensitif. Fizikal ICT ditakrifkan sebagai aset, bangunan dan peralatan yang digunakan di semua bahagian di UKAS. Ia bertujuan untuk mencegah, mengesan, melengah dan mengambil tindakan kepada semua bentuk ancaman yang boleh atau berkeupayaan untuk mengancam di sesebuah bangunan kerajaan.

7.2 Dasar keselamatan Fizikal ICT UKAS

Dasar Keselamatan Fizikal ICT UKAS termaktub di dalam arahan-arahan keselamatan yang terdapat dalam Manual Keselamatan Fizikal setiap bahagian dan cawangan UKAS serta Buku arahan Keselamatan Kerajaan (Buku Hitam).

8.0 KAWALAN KESELAMATAN PERSONEL

8.1 Pengenalan

Personel merupakan aset ICT yang penting. Adalah mustahak bagi semua personel memahami dasar-dasar ICT keselamatan UKAS supaya semua peraturan yang berkaitan dipatuhi bagi memastikan keselamatan ICT terjamin.

8.2 Dasar Keselamatan Personel

Semua personel hendaklah mengikuti semua arahan-arahan dan peraturan keselamatan personel yang termaktub di dalam Buku Arahan Keselamatan Kerajaan (Buku Hitam).

9. KAWALAN KESELAMATAN DOKUMEN / MEDIA

9.1. Pengenalan

Kawalan Keselamatan Dokumen/Media adalah bertujuan untuk melindungi semua bentuk maklumat elektronik dan fizikal bagi menjamin keselamatan maklumat tersebut dari pemusnahan, penyalahgunaan serta kebolehsediaan mencapai semula.

9.2 Keselamatan Dokumen / Media

i. Semua dokumen ICT hendaklah disimpan di bilik khusus iaitu kabinet besi dan laci berkunci dibawah kawalan pegawai yang dipertanggungjawab.

ii. Pergerakan dokumen ICT hendaklah dikawal melalui buku dispatch, borang kawalan dan ID Pengguna.

iii. Semua dokumen ICT tidak boleh dipinda, dibuat penyalinan semula, diedarkan atau digunakpakai oleh mana-mana pihak kecuali dengan kebenaran oleh pegawai yang diberi kuasa (ID Pengguna).

9.3. Media Penyimpan

i. Media penyimpan data dibuat dalam bentuk cakera padat, disket, pita katrij, DASD (data access storage device) dan juga fizikal dokumen. Media penyimpanan dalam jumlah kuantiti data yang besar dan disimpan dengan tepat dan betul.

ii. Semua media penyimpanan rekod disimpan di rak-rak, kabinet atau laci berkunci yang dikhaskan mengikut sistem kawalannya yang tersendiri.

iii. Langkah-langkah kawalan keselamatan bagi memastikan media magnetik dipatuhi:-

a. *Encrypt* semua maklumat rahsia rasmi atau maklumat terperingkat pada setiap media storan.

b. Mengadakan kawalan keselamatan fizikal bagi media storan untuk pegawai-pegawai yang diberi kuasa (authorize) dalam menguruskan penyimpanan dan capaian semula dokumen.

c. Mengadakan rekod rasmi bagi pegawai membuat capaian bagi setiap maklumat yang dikeluarkan.

d. Mengadakan kawalan capaian bagi fail backup dan lain-lain proses penyalinan semual fail.

e. Mengadakan media indeks untuk pengenalan (identification) dengan arahan bagi kerja-kerja khas jika perlu.

iv. Adalah penting fail-fail yang telah diarkibkan disimpan dalam susunan yang sempurna. Setiap fail tersebut hendaklah diterbitkan dalam satu nombor siri

kawalan. Kaedah pengisihan yang digunakan serta tarikh tempoh tamat dokumen-dokumen tersebut mestilah dicatitkan.

9.4. Permusnahan Media

i. Semua pemusnahan dokumen adalah tertakluk mengikut jadual pemusnahan oleh Arkib Negara.

ii. Semua dokumen fizikal yang tidak disimpan sebagai rekod hendaklah dimusnahkan dengan mesin perincih, atau pembakaran dan pastikan tidak boleh digunakan semula.

iii. Untuk memusnahkan media penyimpanan dalam bentuk cakera padat, cakera optic (OD), disket, pita katrij, dan DASD akan melalui proses memadam data dari magnetic ICT media contohnya ‘strong permanent magnets ‘ dan ‘electric degausser’.

iv. Semua aktiviti permusnahan yang tersebut di atas hendaklah direkodkan bagi menyediakan audit trail.

10.0. KESINAMBUNGAN URUSAN, TERMASUK PELAN KONTINGENSI / STRATEGI DAN PELAN PEMULIHAN BENCANA

10.1. Pengenalan

Pelan Kontingensi dan Strategi Kesinambungan Urusan (Business Continuity Strategy) seharusnya ada untuk menjamin kesinambungan dan kejayaan suatu organisasi. Semua aset komputer termasuk data-data amat penting dalam memastikan operasi dan urusan transaksi harian UKAS berjalan lancar.

10.2. Backup

Backup dilakukan bagi memastikan data-data dapat dipulihkan semula apabila berlaku bencana. Semua cawangan dan data centre hendaklah melakukan aktiviti backup mengikut jadual yang telah ditetapkan.

10.3. Pelan Pemulihan Bencana

Pelan Pemulihan Bencana perlu disediakan sebagai panduan memulihkan sistem dalam masa yang dikehendaki dan tersingkat. Pelan ini menerangkan tindakan, bahan-bahan dan sumber-sumber yang diperlukan untuk memulihkan sepenuhnya sistem produksi dan operasi komputer. Bagi memastikan kesinambungan urusan UKAS, semua pihak yang terbabit perlu mengikuti prosedur yang telah dinyatakan didalam pelan tersebut.

11.0 DASAR PENGGUNAAN PERKHIDMATAN LUAR (OUTSOURCING)

11.1. Pengenalan

Penggunaan perkhidmatan luar adalah suatu perjanjian di antara pihak UKAS dengan pihak ketiga iaitu pembekal yang bertanggungjawab melaksanakan fungsi sistem maklumat dan memenuhi kriteria yang telah ditetapkan.

11.2. Keperluan keselamatan

Setiap pegawai mestilah mahir dalam bidang masing-masing. Setiap perubahan yang dibuat pada sistem komputer hendaklah dimaklumkan dan disertakan dengan dokumen bertulis kepada Sektor Pengurusan Korporat, Ketua Pegawai Sistem Maklumat dan Ketua Juruaudit. Keperluan keselamatan boleh dilihat daripada beberapa aspek, antaranya:-

- Sumber manusia
- Keselamatan data
- Keselamatan peralatan dan perisian
- Kawalan kemasukan sistem
- Ketepatan masa

Polisi keselamatan berkaitan dengan perkhidmatan luar adalah:

i. Memastikan pembekal yang dipertanggungjawabkan mempunyai kelayakan dalam bidang berkaitan dan pembekal tempatan yang berdaftar dengan kementerian kewangan.

ii. Menentukan bahagian yang boleh dimasuki / dilawati oleh pihak pembekal yang berhubungkait dengan bidang tugas yang telah dikenal pasti..

iii. Memastikan pihak pembekal mematuhi setiap syarat yang termaktub dalam perjanjian.

iv. Memberikan maklumat yang lengkap dan jelas kepada pembekal untuk pembangunan sistem.

v. Pihak pembekal hendaklah memberikan senarai nama kakitangan mereka yang terlibat dengan projek.

vi. Sebarang pertukaran/penambahan terhadap senarai kakitangan dari pihak pembekal harus dimaklumkan dari masa ke masa.

vii. Pegawai yang terlibat hendaklah memastikan maklumat yang diberikan kepada pembekal tidak disalahgunakan.

viii. Sebarang kecurian, kerosakan dan penyalahgunaan peralatan, perisian atau aplikasi mesti dilaporkan dengan segera kepada jabatan dan pembekal.

ix. Pembekal memberikan senarai sub kontraktor yang terlibat dalam pelaksanaan projek.

x. Semua peralatan dan perisian perlu mempunyai sistem inventori yang sentiasa dikemaskini dan direkodkan pemiliknya.

xi. Mengadakan kaedah laporan terhadap isu-isu/masalah sekiranya ia timbul dari masa ke masa. Contohnya laporan aktiviti/fail log dan masalah dibentangkan dalam mesyuarat yang berkaitan.

xii. Tugas dan tindakan yang tidak dapat diselesaikan harus didokumenkan dan diberi kepada jabatan untuk tindakan susulan.

xiii. Sebarang perisian yang digunakan mesti mempunyai lesen perisian. Dan lesen tersebut mestilah di atas nama Jabatan Unit Kerjasama Awam Swasta.

Dasar penggunaan perkhidmatan luar perlu mempunyai kaedah yang sentiasa dikemaskini dari masa ke masa dengan persetujuan kedua-dua pihak.

12.0 KAWALAN PERUBAHAN

12.1. Pengenalan

Kawalan perubahan diperlukan untuk mengawal dan melindungi integrasi sistem pemprosesan maklumat di UKAS. Prosedur kawalan perubahan harus meliputi perubahan kepada perkakasan, perisian dan manual prosedur sama ada ia secara berjadual atau dalam masa-masa kecemasan.

12.2. Maklumbalas

Semua perubahan yang melibatkan keselamatan perlu dimaklumkan kepada pihak pengurusan dalam bentuk laporan untuk tindakan selanjutnya. Laporan ini hendaklah difailkan.

12.3. Perubahan Kepada Dasar Keselamatan ICT

Satu kajian semula perlu dibuat bagi menyemak dasar yang sedang dilaksanakan. Kajian semula ini perlu dibuat apabila didapati ada perkara yang terdapat dalam dokumen tidak releven dengan teknologi, perundangan dan lain-lain. Kekerapan kajian ini bergantung kepada perubahan yang berlaku dan secepat-cepatnya setahun selepas pelaksanaannya. Hasil kajian semula berbentuk laporan kajian semula sahaja dan tidak semestinya berakhir dengan perubahan dasar sediada.

BAHAN RUJUKAN

1. Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMis) - MAMPU

2. Pekeliling Am Bil 3/2000 : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Maklumat Kerajaan.

3. Buku Arahan Keselamatan (Buku Hitam)

4. MIS Training Institute Information Security Policy

5. Dasar Keselamatan ICT Versi 4.0, Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri, 30 Mac 2006.