UNIVERSITI
MALAYSIA
KELANTAN

Dasar Keselamatan ICT Universiti

Unit Keselamatan, Penyelidikan & Inovasi
Jabatan Teknologi Maklumat & Komunikasi
Universiti Malaysia Kelantan

Julai 2010 versi 3

ISI KANDUNGAN

[*bahagian muka surat ini sengaja dibiarkan kosong*]

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat & Komunikasi (ICT) Universiti. Dasar ini juga menerangkan kepada semua pengguna di UMK mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Universiti. Dasar ini dibuat berdasarkan kepada **Pekeliling Am Bilangan 3 Tahun 2000** bertajuk **"Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"** dan **Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)** yang telah dikeluarkan oleh MAMPU

OBJEKTIF

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

MATLAMAT

Matlamat Utama Dasar Keselamatan ICT Universiti adalah tidak terhad seperti berikut :-

i. memastikan aset ICT dilindungi secukupnya dari perbuatan salahguna atau kecurian / kehilangan;
ii. meminimumkan risiko ke atas aset ICT
iii. memastikan kelancaran operasi harian aset ICT; dan
iv. melindungi kepentingan pihak-pihak bergantung kepada aset ICT daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan dan aksesibiliti aset ICT.

SKOP

Dasar ini meliputi semua aset ICT yang digunakan seperti :-

i. <u>Maklumat</u>
Aset yang digunakan untuk menyokong tadbir urus perkhidmatan Universiti yang melibatkan media storan, prosesan atau penghantaran data, dan juga data itu sendiri. Aset Maklumat termasuk sistem-sistem aplikasi, sistem-sistem pengoperasian, perisian utiliti, sistem-sistem komunikasi, data (sama ada dalam bentuk mentah, ringkasan atau ditafsirkan) dan perkakasan yang berkaitan dengan komputer seperti pelayan, komputer mudah alih, perkakasan komunikasi dan lain-lain perkakasan yang digunakan untuk menyokong urusan perkhidmatan Universiti.

ii. <u>Komunikasi</u>
Gabungan perkakasan telekomunikasi, alat-alat transmisi, video elektronik dan perkakasan audio, perkakasan mengkod dan mentafsir kod, komputer peribadi, prosesan data atau sistem-sistem storan, sistem-sistem komputer, komputer pelayan, rangkaian-rangkaian komputer, alat-alat input/output dan penyambungannya, dan rekod-rekod komputer, program, software dan dokumentasi yang berkaitan yang menyokong perkhidmatan komunikasi.

iii. <u>Dokumentasi</u>
Semua dokumentasi (manual dan prosedur) yang mengandungi maklumat berkaitan dengan spesifikasi teknikal (termasuk dan tidak terhad kepada kod sumber, struktur dan

kamus data), penggunaan elektronik. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, transperencies, risalah dan slaid.

iv. Premis Komputer dan Komunikasi
Semua premis yang digunakan untuk menempatkan aset ICT i) – iii) di atas.

Dasar ini adalah terpakai oleh semua pengguna di UMK termasuk kakitangan, pembekal, pakar runding dan pihak sumber luar yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Universiti.

PRINSIP-PRINSIP

Prinsip yang menjadi asas kepada Dasar Keselamatan ICT Universiti dan hendaklah dipatuhi adalah seperti berikut :-

a. **Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya dibenarkan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermaksud akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan akses adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut

i. Klasifikasi Maklumat – hendaklah mematuhi "**Arahan Keselamatan Kerajaan**" perenggan 53, muka surat 15.;
ii. Tapisan Keselamatan Pengguna – siasatan yang menunjukkan tiada sebab atau faktor untuk menghalang kebenaran mengakses kategori maklumat tertentu;

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, mengemas kini, 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 di bawah kawalannya. Tanggungjawab ini hendaklah dinyatakan dengan jelas sejajar dengan tahap sensitiviti sesuatu aset ICT berkenaan.

d. **Pengasingan**

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada akses yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara bahagian operasi dan rangkaian.

e. **Pengauditan**

Pengauditan adalah 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 atau jejak audit.;

f. **Pematuhan**

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

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 penduaan dan mewujudkan pelan pemulihan bencana / kesinambungan perkhidmatan.; dan

h. **Saling Bergantungan**

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

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 01 : DASAR KESELAMATAN ICT UNIVERSITI

Dasar Keselamatan ICT

Objektif : Mengambil langkah-langkah persediaan bagi perlindungan keselamatan aset ICT dan mengurangkan impak akibat perlanggaran atau bencana yang berlaku.

Pelaksanaan Dasar

1. Pelaksanaan Dasar ini akan dijalankan oleh Naib Canselor selaku Pengerusi Jawatankuasa Pemandu ICT Universiti (JPICTU) dibantu oleh staf JTMK yang terdiri daripada :
   1.1. Pengarah ICT ;
   1.2. Pegawai Keselamatan ICT (ICTSO);
   1.3. Pentadbir Sistem ICT; dan
   1.4. Semua Pegawai Teknologi Maklumat.

Tindakan : Naib Canselor

Penyebaran Dasar

2. Dasar ini perlu disebarkan kepada semua pengguna UMK (termasuk kakitangan, pembekal, pakar runding dan sebagainya)

Tindakan : ICTSO

Penyelenggaraan Dasar

3. Dasar Keselamatan ICT Kerajaan 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 Universiti :

   3.1. kenalpasti dan tentukan perubahan yang diperlukan;
   3.2. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Universiti (JPICTU);
   3.3. perubahan yang dipersetujui oleh JPICTU hendaklah dimaklumkan kepada semua pengguna; dan
   3.4. dasar ini hendaklah dikaji semula sekurang-kurang sekali setahun (apabila perlu).

Tindakan : ICTSO

Pengecualian Dasar

4. Dasar Keselamatan ICT Universiti adalah terpakai kepada semua pengguna ICT UMK dan tiada pengecualian diberikan

Tindakan : Pengarah ICT

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 02 : PENGURUSAN KESELAMATAN ICT UNIVERSITI

Struktur Organisasi Pengurusan Keselamatan ICT Universiti

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.

Naib Canselor

5. Peranan dan tanggungjawab Naib Canselor adalah seperti berikut :

Tindakan : Naib Canselor

5.1. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Universiti;
5.2. memastikan semua pengguna mematuhi dan tertakluk kepada Dasar Keselamatan ICT Universiti;
5.3. memastikan semua keperluan organisasi (sumber kewangan, kakitangan dan perlindungan keselamatan) adalah mencukupi;
5.4. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Universiti; dan
5.5. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Universiti;

JPICTU

6. Tugas dan tanggungjawab JPICTU adalah seperti berikut:

Tindakan : Pengarah ICT

6.1. menentukan halatuju keselamatan ICT Universiti
6.2. membangun pelan dan dasar keselamatan ICT Universiti;
6.3. menyenarai isu-isu keselamatan ICT mengikut keutamaan, yang dihadapi oleh Universiti;
6.4. menyedia cadangan tindakan keselamatan ICT termasuk sumber yang diperlukan bagi melaksanakan cadangan-cadangan tersebut;
6.5. menyenarai teknologi bagi menghadapi ancaman keselamatan ICT;
6.6. membangun program latihan dan pembudayaan keselamatan ICT; dan
6.7. membangun mekanisma menangani insiden bagi permasalahan keselamtan ICT.

Pengarah ICT

Tindakan : Pengarah ICT

7. Ketua Jabatan Teknologi Maklumat & Komunikasi (JTMK) adalah merupakan Pengarah ICT Universiti. Peranan dan tanggungjawab Pengarah ICT adalah seperti berikut :

7.1. membantu Naib Canselor dalam melaksanakan tugas-tugas melibatkan keselamatan ICT;
7.2. menentukan keperluan keselamatan ICT;
7.3. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;
7.4. menentukan tindakan tatatertib yang perlu diambil ke atas pengguna yang telah dikenalpasti melanggar Dasar Keselamatan ICT Universiti;
7.5. memastikan semua warga UMK memahami dan mematuhi Dasar Keselamatan ICT Universiti;
7.6. mengkaji semula dan melaksana kawalan keselamatan ICT selaras dengan keperluan Universiti;
7.7. menentukan kawalan akses semua pengguna terhadap aset ICT Universiti;
7.8. melaporkan penemuan mengenai pelanggaran Dasar Keselamatan ICT kepada ICTSO; dan
7.9. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Universiti.

Pegawai Keselamatan ICT (ICTSO)

Tindakan : ICTSO

8. Pegawai di Unit Keselamatan, Penyelidikan dan Inovasi JTMK adalah merupakan Pegawai Keselamatan ICT (ICTSO) Universiti. Peranan dan tanggungjawab beliau adalah tidak terhad seperti berikut :

8.1. mengurus keseluruhan program-program keselamatan ICT Universiti;
8.2. menguatkuasa Dasar Keselamatan ICT Universiti;
8.3. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Universiti kepada semua pengguna;
8.4. mewujud garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Universiti;
8.5. menjalankan pengurusan risiko;
8.6. menjalankan audit, mengkaji semula, merumus tindakan kepada pengurusan Universiti berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
8.7. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
8.8. melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada Pengarah ICT;
8.9. bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;
8.10. menyiasat dan mengenalpasti pengguna yang melanggar

Dasar Keselamatan ICT Universiti; dan

8.11. Menyedia dan melaksana program-program kesedaran mengenai keselamatan ICT

[*bahagian muka surat ini sengaja dibiarkan kosong*]

9. Pegawai Teknologi Maklumat di Bahagian Aplikasi dan Bahagian Teknikal & Operasi merupakan Pentadbir Sistem ICT Universiti. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut :

Pentadbir Sistem ICT

Tindakan : JTMK

9.1. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;
9.2. menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat, sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT Universiti;
9.3. memantau aktiviti akses harian pengguna;
9.4. mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
9.5. menyimpan dan menganalisas rekod jejak audit; dan
9.6. menyediakan laporan mengenai aktiviti akses kepada pemilik maklumat berkenaan secara berkala.

10. Pemilik Sistem merupakan Pusat Tanggungjawab yang bertanggungjawab terhadap sesuatu sistem. Peranan Pemilik Sistem adalah seperti berikut :

Pemilik Sistem

Tindakan : Pemilik Sistem

10.1. memastikan sistem beroperasi dengan baik dan lancar;
10.2. memastikan segala data dan maklumat di dalam sistem adalah tepat, lengkap dan boleh dipercayai; dan
10.3. memastikan sistem telah dilengkapi dengan langkah-langkah keselamatan melalui semakan senarai kawalan akses dan sebagainya.

11. Peranan Kaunter Perkhidmatan *Help Desk* adalah tidak terhad seperti berikut :

Kaunter Perkhidmatan *Help Desk*

Tindakan : JTMK

11.1. menjadi tempat rujukan dan melaporkan sekiranya berlaku masalah dan isu-isu berkaitan insiden keselamatan ICT; dan
11.2. menjadi Pusat Informasi Insiden Keselamatan ICT Universiti;

Pengguna

Tindakan : Warga UMK

12. Pengguna adalah merupakan semua warga Universiti. Peranan dan tanggungjawab pengguna adalah seperti berikut :

    12.1. membaca, memahami dan mematuhi Dasar Keselamatan ICT Universiti;
    12.2. mengetahui dan memahami implikasi keselamatan ICT serta kesan dari tindakannya;
    12.3. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat Universiti;
    12.4. melaksanakan langkah-langkah perlindungan seperti berikut :
        (a) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
        (b) memeriksa maklumat dan menentukan maklumat tersebut tepat dan lengkap dari semasa ke semasa;
        (c) menentukan kesahihan dan kesediaan maklumat untuk digunakan;
        (d) menjaga kerahsiaan kata laluan;
        (e) mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.
        (f) memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
        (g) menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.
    12.5. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengarah ICT, ICTSO atau Pentadbir Sistem ICT dengan segera;
    12.6. menghadiri program-program kesedaran mengenai keselamatan ICT;
    12.7. bertanggungjawab ke atas aset ICT di bawah kawalannya; dan
    12.8. menandatangani surat akuan pematuhan Dasar Keselamatan ICT Universiti.

Pihak Ketiga

Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.

Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Tindakan : Pengarah ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

13. Akses kepada aset ICT Universiti perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan :

    13.1. Dasar Keselamatan ICT Universiti;
    13.2. Tapisan Keselamatan;
    13.3. Perakuan Akta Rahsia Rasmi 1972; dan
    13.4. Hak Harta Intelek

Nota Rujukan

- 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"

Kawalan Pindaan

Objektif : Mengemaskini Dasar Keselamatan ICT Universiti bagi memastikan keselamatan aset ICT selari dengan perubahan masa dan keperluan serta perkembangan teknologi ICT terkini.

Pindaan Kepada Dasar

Tindakan : Pengarah ICT / ICTSO

14. Berikut merupakan prosedur yang hendaklah diikuti untuk membuat sebarang pindaan kepada dasar:

    14.1. Sebarang pindaan yang hendak dibuat kepada Dasar Keselamatan ICT hendaklah dilakukan dengan menulis secara rasmi kepada Pengarah ICT atau ICTSO. Pindaan-pindaan tersebut akan dibawa ke mesyuarat JPICTU untuk diluluskan;
    14.2. Sebarang pindaan kepada Dasar Keselamatan mestilah dihebahkan kepada semua pengguna. Cara hebahan bolehlah dilakukan melalui risalah, pekeliling, e-mail, atau paparan di laman web Universiti;
    14.3. ICTSO adalah bertanggungjawab menyimpan semua pindaan dan memasukkan pindaan-pindaan tersebut ke dalam Dasar Keselamatan ICT Universiti; dan
    14.4. Dokumen ini adalah dikaji semula setiap enam bulan sekali oleh Pasukan Pengurusan Keselamatan ICT Universiti.

Pemberitahuan Pindaan

Tindakan : ICTSO

15. Sebarang maklum balas, pertanyaan atau pindaan kepada dasar ini hendaklah diajukan kepada ICTSO:

Nama : Pegawai Keselamatan ICT Universiti
Alamat : Unit Keselamatan, Penyelidikan & Inovasi
Jabatan Teknologi Maklumat & Komunikasi
Universiti Malaysia Kelantan,
Karung Berkunci 36, Pengkalan Chepa,
16100 Kota Bharu, Kelantan.
No. Telefon : +609 – 771 7173
No Fax : +609 – 771 7172
e-Mel : fadli@umk.edu.my

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 03 : PENGURUSAN ASET

Akauntabiliti Aset

Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Universiti.

16. Semua aset ICT Universiti hendaklah direkodkan : **Inventori Aset**

    16.1. Ini termasuklah mengenalpasti, mengkategorikan aset dan merekodkan maklumat seperti pemilik, lokasi dan sebagainya; dan — Tindakan : JTMK

    16.2. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya — Tindakan : Warga UMK

Pengelasan dan Pengendalian Maklumat

Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

17. Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen **Arahan Keselamatan Kerajaan** seperti berikut : **Pengelasan Maklumat** — Tindakan : Warga UMK

    17.1. Rahsia Besar;
    17.2. Rahsia;
    17.3. Sulit; atau
    17.4. Terhad.

18. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambilkira langkah-langkah keselamatan berikut : **Pengendalian Maklumat** — Tindakan : Warga UMK

    18.1. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
    18.2. memeriksa maklumat dan memastikan maklumat adalah tepat dan lengkap dari semasa ke semasa;
    18.3. menentukan maklumat sedia untuk digunakan;
    18.4. menjaga kerahsiaan kata laluan;
    18.5. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
    18.6. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

20.7. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 04 : KESELAMATAN SUMBER MANUSIA

Keselamatan ICT Dalam Tugasan Harian

Objektif : Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Universiti

19. Tanggungjawab Keselamatan :

Tanggungjawab Keselamatan

Tindakan : Warga UMK

19.1. Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak; dan

19.2. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam tugas harian.

20. Terma dan syarat Perkhidmatan UMK adalah seperti berikut :

Terma dan Syarat Perkhidmatan

Tindakan : Warga UMK

20.1. warga UMK yang akan dilantik hendaklah mematuhi :
   (a) menandatangani surat akuan Pemantuhan Dasar Keselamatan ICT Universiti; dan
   (b) melepasi Tapisan Keselamatan.

20.2. semasa perkhidmatan, warga UMK tertakluk kepada Surat Akujanji dan **Akta 605 – Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000**; dan

20.3. memulangkan semua aset ICT di bawah kawalannya kepada UMK.

21. Warga UMK yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan **Akta Rahsia Rasmi 1972**.

Perakuan Akta Rahsia Rasmi

Tindakan : Warga UMK

Menangani Insiden Keselamatan ICT

Objektif : Meminimumkan kesan insiden keselamatan ICT

22. Insiden keselamatan ICT adalah perlu dilaporkan kepada ICTSO atau Pengurus ICT dengan kadar segera :

Pelaporan Insiden

Tindakan : Warga UMK

22.1. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

22.2. sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

22.3. kata lalaun atau mekanisma kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
22.4. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan kesilapan komunikasi;
22.5. berlaku percubaan menceroboh, penyelewangan dan insiden-insiden yang tidak tidak diingani.

Nota Rujukan
- Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisma Pelaporan Insiden Keselamatan ICT"; dan
- Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi maklumat dan Komunikasi (ICT) Sektor Awam".

Pendidikan

Objektif : Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT

Program Kesedaran Keselamatan ICT

Tindakan : ICTSO

23. Program Kesedaran Keselamatan ICT
23.1. Setiap pengguna di UMK perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka
23.2. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT Universiti.

Tindakan Tatatertib

Objektif : Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT Universiti.

Pelanggaran Dasar

Tindakan : Warga UMK

24. Pelanggaran Dasar Keselamatan ICT Universiti akan dikenakan tindakan tatatertib berdasarkan **Akta 605 – Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000**.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Kawasan

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

Perimeter Keselamatan Fizikal

25. Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut :-

Tindakan : Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.

25.1. kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
25.2. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
25.3. memperkukuhkan dinding, siling dan lantai;
25.4. menghadkan jalan keluar masuk;
25.5. mengadakan kaunter kawalan, kad pintar, kamera litar tertutup (CCTV) dan sebagainya;
25.6. menyediakan tempat atau bilik khas untuk pelawat; dan

Kawalan Masuk Fizikal

26. Kawalan Masuk Fizikal hendaklah tidak terhad seperti berikut :-

Tindakan : Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.

26.1. setiap staf di UMK hendaklah memakai atau mengenakan kad staf sepanjang waktu bertugas;
26.2. setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan;
26.3. kehilangan pas pelawat mestilah dilaporkan dengan segera kepada Pengawal Keselamatan;
26.4. hanya staf dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu jabatan.

Kawasan Larangan

27. 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. Akses kepada kawasan larangan hanya kepada pegawai-pegawai yang diberikan kuasa sahaja :

Tindakan : Pegawai Keselamatan Universiti, Pengarah ICT dan ICTSO.

27.1. secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu;

29.2. pihak ketiga adalah dilarang sama sekali untuk memasuki kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas berkenaan selesai; dan

29.3. semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Naib Canselor

Keselamatan Kelengkapan

Objektif : Melindungi peralatan dan maklumat

Peralatan

Tindakan : Warga UMK

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

28.1. setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;

28.2. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;

28.3. setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan

28.4. sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO dan Pengarah ICT

Media Storan

Tindakan : Warga UMK

29. Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar, Langkah-langkah pencegahan seperti berikut hednagklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat

29.1. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

29.2. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;

29.3. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan

29.4. pergerakan media storan hendaklah direkodkan.

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

Kabel

Tindakan : JTMK dan ICTSO

30.1. menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
30.2. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan
30.3. melindungi laluan pemasangan kabel sepenuhnya

Keselamatan Komunikasi & Operasi

Objektik : Meminimumkan risiko keselamatan akibat kegagalan kelengkapan beroperasi yang telah ditetapkan.

31. Perkakasan hendaklah disenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti :

Penyelenggaraan

Tindakan : JTMK

33.1. semua perkakasan yang disenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;
33.2. perkakasan hanya boleh disenggarakan oleh staf atau pihak yang dibenarkan sahaja;
33.3. semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan
33.4. semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT berkenaan; dan
33.5. semua aktiviti penyelenggaraan perlu direkodkan di dalam borang harta modal.

32. Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada kepada pelbagai risiko. Langkah-langkah berikut tidak terhad hendaklah diambil untuk menjamin keselamatan perkakasan :

Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat

Tindakan : Warga UMK

32.1. peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan Pengarah ICT dan tertakluk kepada tujuan yang dibenarkan; dan
32.2. aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.

33. Bagi perkakasan yang dibawa keluar dari premis UMK, langkah-langah keselamatan hendaklah diadakan dengan mengambilkira risiko yang wujud di luar kawalan UMK :

Perkakasan di Luar Premis

Tindakan : Warga UMK

33.1. peralatan perlu dilindungi dan dikawal sepanjang masa; dan
33.2. penyimpanan atau penempatan peralatan mestilah mengambilkira langah-langkah keselamatan yang bersesuaian.

Perlupusan

Tindakan : JTMK

34. Aset ICT yang akan dilupuskan hendaklah melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan UMK :

    34.1. semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran; dan
    34.2. sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan.

Nota Rujukan
Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer".

Clear Desk dan Clear Screen

Tindakan : Warga UMK

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

    35.1. gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan
    35.2. bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.

Keselamatan Persekitaran

Objektif : Melindungi aset ICT Universiti dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian dan kemalangan.

Kawalan Persekitaran

Tindakan : ICTSO

36. 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 **Jabatan Pembangunan, Infra dan Perkhidmatan (JPIP)**. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut perlu diambil :

    36.1. merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
    36.2. 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;

38.3. peralatan perlindungan seperti perlindungan kebakaran atau kilat / petir hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
38.4. bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
38.5. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
38.6. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan
38.7. 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.

37. Bekalan Kuasa : **Bekalan Kuasa**

37.1. semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai; Tindakan : Pengarah ICT
37.2. 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
37.3. semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

38. Prosedur Kecemasan : **Prosedur Kecemasan**

38.1. setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada **Surat Pekeliling Am Bilangan 4 Tahun 2006** bertajuk **"Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam"**; dan Tindakan : Pengarah ICT
38.2. kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Universiti yang dilantik mengikut aras.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 06 : PENGURUSAN OPERASI & KOMUNIKASI

Pengurusan Prosedur Operasi

Objektif : Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.

39. Pengendalian Prosedur adalah tidak terhad seperti berikut : **Pengendalian Prosedur**

    39.1. semua prosedur keselamatan ICT yang diwujud, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal; Tindakan : Pengarah ICT
    39.2. 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;
    39.3. semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan; dan
    39.4. semua staf UMK hendaklah mematuhi prosedur yang telah ditetapkan.

40. Kawalan Perubahan hendaklah tidak terhad seperti berikut : **Kawalan Perubahan**

    40.1. pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pengurus ICT terlebih dahulu; Tindakan : JTMK
    40.2. aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik komputer atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
    40.3. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
    40.4. semua aktiviti perubahan atau pengubahsuaian hendakalah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak.

Prosedur Pengurusan Insiden

Tindakan : ICTSO

41. Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambilkira kawalan-kawalan berikut :-

    41.1. mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
    41.2. menyedia pelan kontigensi dan mengaktifkan pelan kesimbungan perkhidmatan;
    41.3. menyimpan jejak audit dan memelihara bahan bukti; dan
    41.4. menyediakan tindakan pemulihan segara.

Perancangan dan Penerimaan Sistem

Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem

Perancangan Kapasiti

Tindakan : Pentadbir Sistem ICT, ICTSO

42. Perancangan Kapasiti hendaklah tidak terhad seperti berikut :

    42.1. kepasiti 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
    42.2. keperluan kapasiti ini perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang

Penerimaan Sistem

Tindakan : Pentadbir Sistem ICT, ICTSO

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

Perisian Berbahaya

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

Perlindungan dari Perisian Berbahaya

Tindakan : Warga UMK

44. Perlindungan dari Perisian Berbahaya tidak terhad :

    44.1. memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti virus dengan penggunaan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat;

46.2. memasang dan menggunajan hanya perisian yang berdaftar dan dilindungi di bawah **Akta Hakcipta (Pindaan) Tahun 1997**;
46.3. mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
46.4. mengemaskini *pattern* anti virus sekerap yang mungkin (sekurang-kurangnya sekali sehari);
46.5. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
46.6. menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
46.7. memasukan klusa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya;
46.8. mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
46.9. memberi amamran mengenai ancaman keselamatan ICT seperti serangan virus.

Housekeeping

Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.

45. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti berikut perlu dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site*.

Penduaan

Tindakan : JTMK

45.1. membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya seklai atau setelah mendapat versi terbaru;
45.2. memberi salinan penduaan ke atas semua data dan maklumat mengikut keperluan ooperasi; dan
45.3. menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada wakti kecemasan.

46. Sistem Log

Sistem Log

Tindakan : JTMK

46.1. mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
46.2. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaikpulih dengan segera; dan

48.3. sekiranya wujud aktiviti-aktiviti tidak sah lain sepertu kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.

Pengurusan Rangkaian

Objektif : Melindungi maklumat dalam rangkaian dan infastruktur sokongan

Kawalan Infrastruktur Rangkaian

Tindakan : JTMK

47. Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman keada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan (tidak terhad) :

    47.1. tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan akses dan pengubahsuaian yang tidak dibenarkan;
    47.2. peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
    47.3. akses kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
    47.4. semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;
    47.5. *firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi serta dikonfigurasi oleh pentadbir sistem;
    47.6. semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan UMK;
    47.7. semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;
    47.8. memasang perisian *Intrusion Detection System* (IDS) atau *Intrusion Prevention System* (IPS) bagi mengensan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UMK;
    47.9. memasang *Web Content Filter* pada *Internet Gateway* untu menyekat aktiviti yang dilarang seperti 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"**;
    47.10. sebarang penyambungan rangkaian yang bukan di bawah kawalan UMK hendaklah mendapat kebenaran ICTSO;
    47.11. semua pengguna hanya dibenarkan menggunakan rangkaian UMK sahaja. Penggunaan modem adalah dilarang sama sekali;

49.12. memastikan keperluan perlindungan ICT adalah bersesuai dan mencukupi bagi menyokkong perlindungan yang lebih optimum; dan
49.13. sebarang penyambungan rangkaian daripada pihak ketiga (*remote tunneling*) ke dalam sistem rangkaian UMK hendaklah mendapat kebenaran ICTSO.

Pengurusan Media

Objektif : Melindungi aset ICT daripada kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

48. Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Naib Canselor terlebih dahulu.

Penghantaran dan Pemindahan

Tindakan : Warga UMK

49. Prosedur Pengendalian Media hendaklah :

Prosedur Pengendalian Media

Tindakan : Warga UMK

49.1. melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
49.2. menghadkan dan menentukan akses media kepada pengguna yang sah sahaja;
49.3. menghadkan pengedaran data atau media untuk tujuan yang dibenarkan;
49.4. mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
49.5. menyimpan semua media di tempat yang selamat; dan
49.6. media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.

50. Keselamatan Sistem Dokumentasi hendaklah :

Keselamatan Sistem Dokumentasi

Tindakan : Pentadbir Sistem ICT, ICTSO

50.1. memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
50.2. menyediakan dan memantapkan keselamatan sistem dokuementasi; dan
50.3. mengawal dan merekodkan semua aktiviti akses sistem dokumentasi sedia ada.

Keselamatan Komunikasi

Objektif : Melindungi aset ICT melalui sistem komunikasi yang selamat

Internet

51. Tatacara penggunaan Internet adalah seperti berikut :

Tindakan : Warga UMK

51.1. laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Naib Canselor;

51.2. bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;

51.3. bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Naib Canselor sebelum dimuat naik ke Internet;

51.4. pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

51.5. sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UMK;

51.6. hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walaubagaimana, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Naib Canselor terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan

51.7. maklumat lanjut mengenai keselamatan Internet boleh dirujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003** bertajuk **"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"**.

Mel Elektronik

52. Tatacara penggunaan Mel Elektronik tidak terhad seperti berikut :

Tindakan : Warga UMK

52.1. akaun atau alamat mel elektronik (e-mel) yang diperuntukan oleh UMK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

52.2. setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh UMK;

52.3. memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

52.4. penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

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

54.6. pengguna hendaklah mengelak daru membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

54.7. pengguna hendaklah mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

54.8. setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpa mengikut tatacara pengurusan sistem fail eletronik yang telah ditetapkan;

54.9. e-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

54.10. pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan

54.11. maklumat lanjut mengenai keselamatan e-mel boleh dirujuk kepada **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003** bertajuk **"Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"**.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 07 : KAWALAN AKSES

Dasar Kawalan Akses

Objektif : Memahami dan mematuhi keperluan dalam mencapai dan menggunakan aset ICT Universiti.

Keperluan Tugas

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

Tindakan : JTMK, ICTSO

Pengurusan Akses Pengguna

Objektif : Mengawal akses pengguna ke atas aset ICT Universiti.

Akaun Pengguna

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

Tindakan : Warga UMK

    54.1. akaun yang diperuntukan oleh Universiti sahaja boleh digunakan;
    54.2. akaun pengguna mestilah unik;
    54.3. akaun pengguna yang di wujud pertama kali akan diberi tahap akses paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
    54.4. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Universiti. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
    54.5. penggunaan akaun milik orang lain atau akauan yang dikongsi bersama adalah dilarang; dan
    54.6. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut :
        (a) pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) bulan;
        (b) bertukar bidang tugas kerja;
        (c) bertukar ke agensi lain;
        (d) bersara; atau
        (e) ditamatkan perkhidmatan.

Jejak Audit

Tindakan : Pentadbir Sistem ICT

55. Jejak Audit

55.1. 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 digunakan;
(b) aktiviti akses penggun 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.

55.2. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan mendapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsiaian yang tidak dibenarkan.

Kawalan Akses Sistem dan Aplikasi

Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk akses yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Sistem Maklumat & Aplikasi

Tindakan : Pentadbir Sistem ICT, ICTSO

56. Akses sistem dan aplikasi di UMK adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan akses sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi :

56.1. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap akses dan sensitiviti maklumat yang telah ditetntukan;

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

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

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

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

56.6. Akses sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walaubagaimana, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja

Peralatan Komputer Mudah Alih

Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.

57. Penggunaan Peralatan Komputer Mudah Alih

Penggunaan Peralatan Komputer Mudah Alih

Tindakan : Warga UMK

57.1. merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan

57.2. komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian

58. Keperluan Keselamatan

Keperluan Keselamatan

Tindakan : Pemilik Sistem, Pentadbir Sistem ICT, ICTSO

58.1. pembangunan sistem hendaklah mengambilkira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh menganggu pemprosesan dan ketepatan maklumat;

58.2. ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukan, sistem pemprosesan untuk menentukan output untuk memastikan data yang telah diproses adalah tepat; dan

58.3. 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.

Kriptografi

Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat

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

Penyulitan

Tindakan : Warga UMK

60. Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara eletronik.

Tandatangan Digital

Tindakan : Warga UMK

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

Pengurusan Kunci

Tindakan : Warga UMK

Fail Sistem

Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

Kawalan Fail Sistem

Tindakan : Pentadbir Sistem ICT

62. Kawalan Fail Sistem

62.1. proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;

62.2. kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;

62.3. mengawal akses ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan

62.4. mengaktifkan aufit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

Pembangunan dan Proses Sokongan

Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi

Kawalan Perubahan

Tindakan : Pentadbir Sistem ICT

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

Hak Harta Intelek

Tindakan : Pentadbir Sistem ICT

64. Semua pembangunan sistem maklumat dan aplikasi hendaklah dipastikan bahawa UMK akan menerima hak pemilikan Kod Sumber (*Source code*) dan hak harta intelek (*Intellectual Property Right* – IP) secara mutlak.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 09 : PENGENDALIAN INSIDEN ICT

Mekanisma Pelaporan

Objektif : Menyalurkan maklumat insiden ICT kepada GCERT untuk mendapat bantuan teknikal untuk tujuan penyelesaian atau pencegahan.

Insiden Keselamatan

65. Insiden keselamatan boleh dikategori tidak terhad kepada kejadian-kejadian seperti berikut :

Tindakan : ICTSO

65.1. percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (*probing*);
65.2. serangan kod jahat (*malicious code*) seperti virus, trojan horse, worms dan sebagainya;
65.3. gangguan yang disengajakan (*unwanted disruption*) atau halangan pemberian perkhidmatan (*denial of service*);
65.4. menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorised access*); dan
65.5. pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

Tanggungjawab Pelapor

66. Tanggungjawab pelapor adalah seperti berikut :

Tindakan : Pengarah ICT / ICTSO

66.1. mengurus tindakan ke atas insiden yang berlaku sehingga keadaan pulih;
66.2. mengaktifkan *Business Resumption Plan* (BRP) jika perlu;
66.3. menentukan samada insiden ini perlu dilaporkan kepada agensi penguatkuasaan Undang-undang / Keselamatan;
66.4. menentukan tahap keutamaan insiden;
66.5. melaporkan insiden kepada GCERT; dan
66.6. mengambil langkah pemulihan awal.

Kaedah Melapor

67. Laporan boleh dibuat menggunakan kaedah-kaedah berikut :

Tindakan : ICTSO

67.1. Mel Elektronik (e-mel)
Alamat e-mel : gcert@mampu.gov.my
67.2. Borang Pelaporan Insiden
Borang boleh diperolehi di laman :
http://gcert.mampu.gov.my
67.3. Telefon hotline
Nombor Telefon : +603 – 8888 3150
67.4. Faks
Nombor faksimili : +603 – 8888 3286

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 10 : PELAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan

Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

Pelan Kesinambungan Perkhidmatan

Tindakan : ICTSO

68. 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 JPICTU dan perkara-perkara berikut perlu diberi perhatian :

    68.1. mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
    68.2. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
    68.3. mendokuemntasikan proses dan prosedur yang telah dipersetujui;
    68.4. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
    68.5. membuat penduaan; dan
    68.6. menguji dan mengemaskini pelan sekurang-kurang setahun sekali.

[*bahagian muka surat ini sengaja dibiarkan kosong*]

[*bahagian muka surat ini sengaja dibiarkan kosong*]

BAHAGIAN 11 : PEMATUHAN

Pematuhan dan Keperluan Perundangan

Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Universiti.

Pematuhan Dasar

Tindakan : Warga UMK

69. Setiap pengguna di UMK hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Universiti dan undang-undang atau peraturan-peraturan lain yang berkaitan dikuatkuasakan. Semua aset ICT di UMK termasuk maklumat yang disimpan didalamnya adalah **Hak Milik Kerajaan** dan Naib Canselor berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Keperluan Perundangan

Tindakan : Warga UMK

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

    70.1. Arahan Keselamatan;
    70.2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
    70.3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
    70.4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”;
    70.5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
    70.6. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk “Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam”;
    70.7. Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk “Tatacara Penyediaan, Penilaian dan Penerimaan Tender”;
    70.8. Surat Pekeliling Bilangan 3 Tahun 1995 bertajuk “Peraturan Perolehan Perkhidmatan Perundingan”;
    70.9. Akta Tandatangan Digital 1997;
    70.10. Akta Jenayah Komputer 1997;
    70.11. Akta Hak cipta (Pindaan) Tahun 1997;
    70.12. Akta Rahsia Rasmi 1972;
    70.13. Pekeliling Am Bilangan 1 Tahun 2006 bertajuk “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”; dan

72.14. Surat Pekeliling Am Bilangan 3 Tahun 2009 bertajuk "Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam".

[bahagian muka surat ini sengaja dibiarkan kosong]