UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

DASAR KESELAMATAN ICT

UNIVERSITI KEBANGSAAN MALAYSIA

KUATKUASA
1 Disember 2014
Kelulusan LPU Bil.4/2014

www.ukm.my/ptm

REKOD PINDAAN

Bil.	Tarikh Pindaan	Ringkasan	Kelulusan	Tarikh kuatkuasa
1.				
2.				

KANDUNGAN

8. KESELAMATAN OPERASI ICT

8.1 Keselamatan Operasi ICT
- 8.1.1 Prosedur Operasi ICT
- 8.1.2 Kawalan Perubahan
- 8.1.3 Pengasingan Tugas dan Tanggungjawab

8.2 Pelindungan daripada *Malware*

8.3 Operasi Rangkaian

8.4 Pemantauan Aktiviti Pemprosesan Maklumat

8.5 *Back up*

9. KAWALAN CAPAIAN

9.1 Dasar Kawalan Capaian

9.2 Pengurusan Capaian Pengguna
- 9.2.1 Pengurusan Kata Laluan

9.3 Kawalan Capaian Rangkaian
- 9.3.1 Capaian Intranet
- 9.3.2 Capaian Internet

9.4 Kawalan Capaian Sistem Pengoperasian

9.5 Kawalan Capaian Sistem Aplikasi

10. PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

11.1 Mekanisme Pelaporan Insiden Keselamatan ICT

11.2 Pengurusan Maklumat Insiden Keselamatan ICT

11. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN ICT

12.1 Pelan Kesinambungan Perkhidmatan ICT

12. PEMATUHAN

12.1 Pematuhan dan Keperluan Perundangan
- 12.1.1 Pematuhan Dasar
- 12.1.2 Pematuhan Terhadap Keperluan Audit
- 12.1.3 Keperluan Perundangan

12.2 Pelanggaran Dasar

LAMPIRAN: Senarai Akta / Peraturan Berkaitan

i. DEFINISI

Definisi berikut digunakan dalam Dasar ini yang berkaitan dengan keselamatan ICT di UKM:

Penyataan	Definisi
Pemilik Aset	Pemilik Aset adalah individu atau entiti yang diberi tanggungjawab untuk mengawal pengeluaran, pembangunan, penyelenggaraan, penggunaan dan keselematan sesuatu aset.
Aset ICT	Aset yang telah dikenalpasti dan mempunyai nilai kepada agensi yang telah dikategorikan seperti berikut: • Perkakasan • Perisian • Perkhidmatan capaian • Perkhidmatan sokongan • Maklumat / data • Sumber manusia
Clear Desk dan *Clear Screen*	Bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya
Media	Meliputi peralatan atau perantara yang digunakan untuk menyimpan data dan maklumat seperti disket, *pen/thumb drive*, cakera padat, cakera keras, alat komunikasi mudah alih, *notebook* dan dokumen bercetak
Pengguna	Terdiri daripada kakitangan, pelajar, pembekal dan pihak-pihak lain yang menggunakan perkhidmatan ICT di UKM
Urusetia Sistem Aplikasi	Pusat Tanggungjawab (PTJ) yang bertanggungjawab menggerakkan pelaksanaan sesuatu sistem aplikasi dan menentukan sebarang perubahan ke atas sistem aplikasi tersebut serta bertanggungjawab ke atas pengwujudan, pengemaskinian dan kesahihan maklumat
Pentadbir *Server*	Pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan *server* dan data yang disimpan
Aktiviti Pemprosesan Maklumat	Proses yang melibatkan peringkat input sehingga menghasilkan output maklumat

ii. SINGKATAN

Singkatan berikut digunakan dalam Dasar ini yang berkaitan dengan keselamatan ICT di UKM:

Singkatan	Perihalan
UKM	Universiti Kebangsaan Malaysia
ICT	Teknologi Maklumat dan Komunikasi
ICTSO	Pegawai Keselamatan ICT
CIO	Ketua Pegawai Maklumat
UKMCERT	UKM *Computer Emergency Response Team*
PTM	Pusat Teknologi Maklumat
PTJ	Pusat Tanggungjawab

1. PENGENALAN

UKM bertanggungjawab untuk menyediakan persekitaran Teknologi Maklumat dan Komunikasi (ICT) yang berintegriti demi kecemerlangan akademik dan kecekapan pentadbiran. Kemudahan ICT yang mencukupi dan selamat adalah penting bagi meningkatkan pengajaran dan pembelajaran, penyelidikan dan pembangunan (R&D). Persekitaran ICT yang selamat juga akan meningkatkan kualiti dan kecekapan pentadbiran serta menjadikan warga universiti yang bermaklumat, berpengetahuan dan berkemahiran untuk membolehkan mereka melaksanakan tugas dan tanggungjawab dengan berkesan bagi mencapai aspirasi universiti.

2. OBJEKTIF KESELAMATAN ICT

Dasar Keselamatan ICT UKM (selepas ini disebut sebagai “Dasar”) diwujudkan untuk menjamin kesinambungan bisnes Universiti dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Universiti. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Objektif Dasar adalah seperti berikut:

(a) Memastikan kelancaran urusan pengoperasian UKM dan meminimumkan kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang menggunakan sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

(c) Mencegah salah guna atau kecurian aset ICT dan

(d) Mewajibkan pematuhan Dasar ke atas setiap pengguna / warga Universiti yang mana sekiranya berlaku ketidakpatuhan

3. PELAKSANAAN, PENYELENGGARAAN DAN PEMAKAIAN DASAR SECARA MANDATORI

3.1 Pelaksanaan Dasar Keselamatan ICT

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Universiti dan perundangan yang berkaitan.

(a) UKM bertanggungjawab memastikan pelaksanaan ini dan syarat yang berkaitan dengan pengguna dan kod etika diamalkan selaras dengan kemudahan di bawah kawalannya; dan

(b) Ketua PTJ bertanggungjawab memastikan Dasar ini diamalkan selaras dengan kemudahan di bawah kawalan dan pengurusannya.

3.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada pengguna dan boleh dicapai melalui portal rasmi Universiti.

3.3 Penyelenggaraan Dasar

Dasar ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Universiti berhak meminda, membatal, mengehad dan menambah mana-mana Dasar ini mengikut kesesuaian dan keperluan semasa.

Penyelenggaraan Dasar adalah tertakluk kepada prosedur berikut:

(a) Dasar ini hendaklah dikaji semula mengikut keperluan semasa;

(b) Kenal pasti dan tentukan perubahan yang diperlukan dan dibincangkan dalam Mesyuarat Jawatankuasa Keselamatan ICT;

(c) Perakuan pindaan dibawa ke Mesyuarat Majlis Teknologi Maklumat untuk pengesahan sebelum diluluskan oleh Lembaga Pengarah Universiti (LPU); dan

(d) Pindaan Dasar yang telah dipersetujui dimaklumkan kepada pengguna.

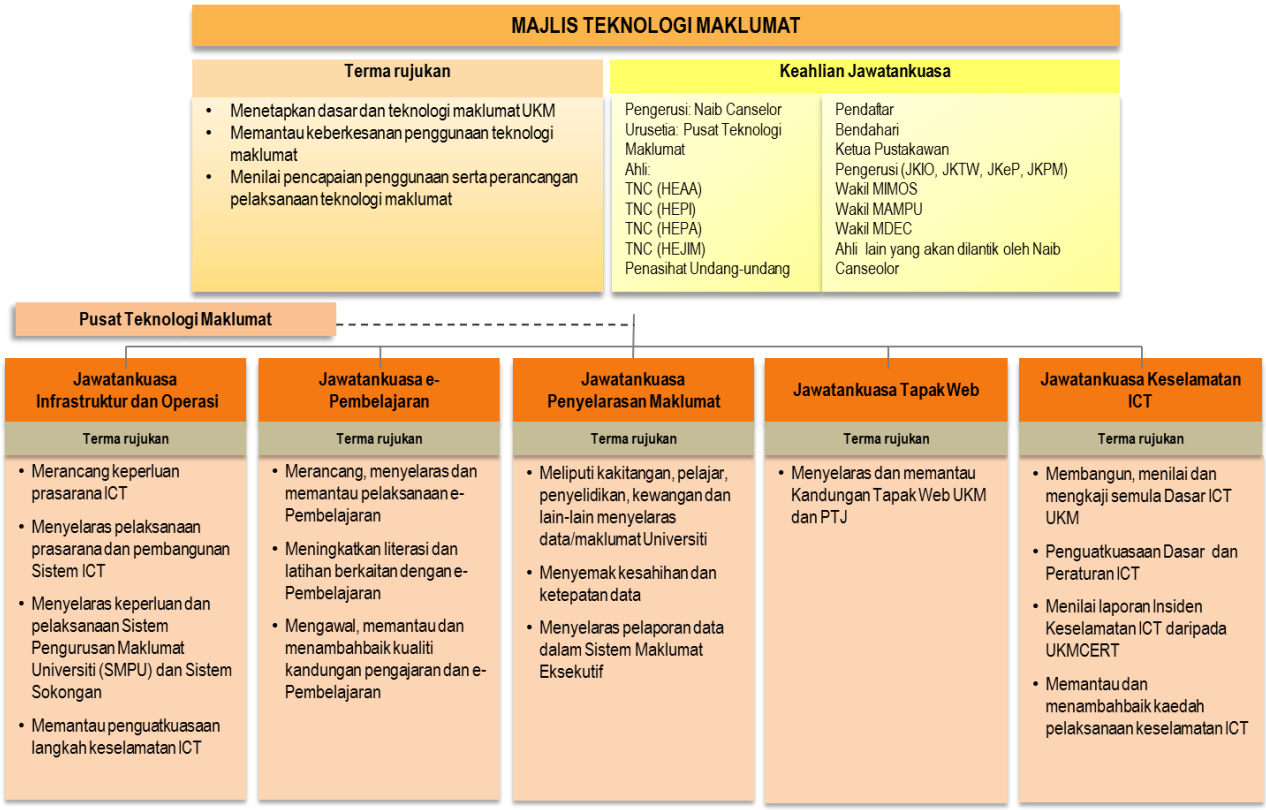
3.4 Pemakaian Dasar Secara Mandatori

Semua pengguna adalah tertakluk kepada pemakaian Dasar ini dan tiada pengecualian diberikan oleh Universiti.

4. ORGANISASI KESELAMATAN ICT

4.1 Majlis Teknologi Maklumat

Majlis Teknologi Maklumat (MTM) dan Jawatankuasa Kerja ditubuhkan dengan terma rujukan seperti berikut:



4.2 Ketua Pegawai Maklumat (CIO)

Pelantikan CIO adalah memenuhi keperluan Pekeliling Ketua Setiausaha Negara (bertarikh 22 Mac 2000). CIO bertanggungjawab untuk:

(a) Memastikan PTJ mematuhi Dasar Keselamatan ICT; dan

(b) Memastikan Dasar ini dikaji semula mengikut keperluan semasa

4.3 Pegawai Keselamatan ICT (ICTSO)

Pelantikan ICTSO adalah memenuhi keperluan Pekeliling Am Bil.3/2010 yang berperanan:

(a) Menguatkuasakan Dasar;

(b) Memantau pematuhan terhadap Dasar;

(c) Memberi penerangan dan kesedaran berkenaan Dasar dan isu berkaitan keselamatan ICT kepada pengguna;

(d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar; dan

(e) Memastikan insiden keselamatan ICT diurus dan dikendalikan dengan berkesan.

4.4 Jawatankuasa Keselamatan ICT UKM

Jawatankuasa ini berperanan untuk merancang pelaksanaan, pemantauan dan penguatkuasaan serta pengemaskinian Dasar. Jawatankuasa ini dipengerusikan oleh ClO dan ICTSO sebagai setiausaha dan keahlian lain dilantik oleh CIO.

Terma rujukan Jawatankuasa Keselamatan ICT adalah seperti berikut:

(a) Menilai semula Dasar ini dari semasa ke semasa;

(b) Menyebar dan menguatkuasakan Dasar kepada warga Universiti dan memantau pematuhannya;

(c) Menerima aduan insiden keselamatan ICT dan menjalankan siasatan teknikal ke atas sebarang pelanggaran Dasar;

(d) Menyediakan laporan insiden keselamatan ICT berdasarkan laporan daripada UKMCERT dan mengemukakan kepada Jawatankuasa Tatatertib Kakitangan bagi kakitangan dan Pihak Berkuasa Tatatertib Pelajar bagi pelajar; dan

(e) Memantau dan menambahbaik kaedah pelaksanaan keselamatan ICT di UKM;

4.5 UKMCERT

Penubuhan UKMCERT adalah memenuhi keperluan GCERT dan Arahan Teknologi Maklumat 2007 untuk memastikan tahap keselamatan ICT adalah terjamin setiap masa.

Terma Rujukan UKMCERT adalah seperti berikut:

(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;

(b) Merekod dan menjalankan siasatan awal insiden yang diterima;

(c) Menangani tindak balas (*respond*) terhadap insiden keselamatan ICT dan mengambil tindakan baik pulih;

(d) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden dapat dielakkan; dan

(e) Melaporkan status tindakan insiden keselamatan kepada Jawatankuasa Keselamatan ICT UKM;

4.6 Pusat Tanggungjawab Teknologi Maklumat

Pusat Tanggungjawab Teknologi Maklumat terdiri daripada Pusat Teknologi Maklumat (Kampus Induk) dan Jabatan Teknologi Maklumat (PPUKM).

Pusat Tanggungjawab Teknologi Maklumat bertanggungjawab memberi dan menyediakan perkhidmatan ICT untuk mencapai kecemerlangan sistem penyampaian perkhidmatan universiti. Selain itu ia juga merupakan entiti yang terlibat secara langsung dalam perancangan dan pelaksanaan aktiviti ICT di Universiti.

(a) Perancangan ICT

i. Perancangan hendaklah memenuhi fungsi dan keperluan UKM dalam pengajaran, pembelajaran, penyelidikan, pentadbiran dan pengurusan; dan

ii. Perancangan hendaklah selaras dengan agenda ICT Negara dan mematuhi Dasar, Peraturan dan Garis Panduan yang ditentukan oleh Kerajaan Malaysia.

(b) Perolehan ICT

i. Semua perolehan hendaklah mematuhi Prosedur Perolehan UKM dan Kerajaan kecuali bagi kes tertentu dengan mendapat perakuan atau kelulusan khas Bendahari UKM;

(c) Pemasangan dan Penyelenggaraan

i. Pemasangan perkakasan dan atau perisian dibekalkan oleh Pusat Tanggungjawab Teknologi Maklumat adalah di bawah penyeliaannya kecuali yang diperolehi oleh PTJ; dan

ii. PTJ hendaklah memastikan perkakasan dan atau perisian ICT di bawah kawalannya diselenggara dengan sempurna.

5. TANGGUNGJAWAB PENGURUSAN, KAKITANGAN UNIVERSITI DAN PIHAK KETIGA

5.1 Tanggungjawab Pengurusan

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

(a) Memastikan semua aset ICT diurus dan dikendalikan dengan mengambil kira semua aspek keselamatan ICT berdasarkan perundangan dan peraturan yang ditetapkan;

(b) Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada kakitangan UKM;

(c) Memastikan tapisan keselamatan terhadap kakitangan yang dikehendaki menguruskan maklumat terperingkat;

(d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pengguna sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan

(e) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksana dan diselenggara oleh pihak ketiga.

5.2 Tanggungjawab Kakitangan Universiti

(a) Membaca, memahami dan mematuhi Dasar;

(b) Mengetahui dan memahami implikasi penggunaan aset ICT terhadap keselamatan ICT dan sebarang pelanggaran akan diambil tindakan disiplin dan/atau undang-undang; dan

(c) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Ketua PTJ / ICTSO dengan segera.

5.3 Tanggungjawab Pihak Ketiga

Pihak ketiga (Pembekal) perlu mematuhi perkara berikut bagi menjamin keselamatan aset ICT yang digunakan:

(a) Membaca, memahami dan mematuhi Dasar;

(b) Memastikan diberi penerangan / taklimat oleh Pusat Tanggungjawab Teknologi Maklumat mengenai keselamatan maklumat dan kemudahan pemprosesan maklumat sebelum diberi kebenaran capaian;

(c) Akses kepada aset ICT UKM perlu berlandaskan kepada perjanjian kontrak yang bersekali dengan Perjanjian Kerahsiaan (*Non Disclosure Agreement*) dan peraturan perundangan yang berkaitan;

(d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam Kontrak; dan

(e) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian/kontrak yang telah ditetapkan.

6. KESELAMATAN FIZIKAL ASET ICT DAN PERSEKITARAN

6.1 Keselamatan Persekitaran

Dasar ini memperuntukkan bahawa aset ICT perlu dilindungi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses fizikal yang tidak dibenarkan.

6.1.1 Kawalan Keselamatan Fizikal

Perkara-perkara berikut perlu dipatuhi:

(a) Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan tahap keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;

(b) Menggunakan keselamatan perimeter (halangan seperti dinding, *access door system*, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

(c) Melaksanakan keselamatan fizikal persekitaran kerja;

(d) Melaksanakan perlindungan fizikal dari kebakaran, banjir dan bencana; dan

(e) Memastikan kawasan penghantaran dan pemunggahan (*loading area*) mematuhi kawalan keselamatan yang ditetapkan;

(f) Mengenalpasti kawasan yang dihadkan kepada personel tertentu sahaja

6.1.2 Kawalan Keluar dan Masuk Fizikal

Kawalan keluar dan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke bangunan. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Semua warga Universiti hendaklah memakai Kad Kampus sepanjang berada di UKM;

(b) Pihak ketiga / pelawat perlu mendapatkan Pas Keselamatan sebelum berurusan dan memulangkan semula selepas selesai urusan;

(c) Mengehadkan laluan keluar masuk dengan mengadakan kaunter kawalan dan kawalan pintu masuk yang bersesuaian; dan

(d) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad (contoh: Bilik Server).

7. PENGURUSAN ASET ICT

7.1 Perancangan Kapasiti Aset ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Kapasiti sesuatu aset ICT (perkakasan, perisian, sumber manusia, kewangan dan lain-lain) hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan

(b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

7.2 Akauntabiliti Aset

Dasar ini memperuntukkan semua aset ICT perlu diberi kawalan dan perlindungan yang bersesuaian oleh pemilik / pemegang aset.

7.2.1 Inventori Aset ICT

Perkara berikut perlu dipatuhi dalam menyokong perlindungan yang bersesuaian ke atas aset ICT:

(a) Memastikan maklumat aset ICT direkodkan dalam Borang Daftar Harta Modal Dan Inventori dan sentiasa dikemaskini;

(b) Memastikan aset ICT mempunyai pemilik yang bertanggungjawab ke atas semua aset ICT di bawah kawalannya dan dikendalikan oleh pengguna yang dibenarkan sahaja;

(c) Memastikan semua aset ICT dikembalikan berdasarkan peraturan yang ditetapkan bagi kakitangan yang tamat perkhidmatan atau bertukar dari Universiti; dan

(d) Menguatkuasakan peraturan bagi pengendalian aset ICT.

7.2.2 Penggunaan Aset ICT

Aset ICT perlu dilindungi daripada kehilangan, kerosakan, kecurian, salah guna, gangguan ke atas peralatan berkenaan dan bisnes utama Universiti. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Setiap PTJ yang menyediakan kemudahan pinjaman perkakasan perlu merekod maklumat peminjaman dan pemulangan dan tempoh pinjaman adalah tertakluk kepada kelulusan Ketua PTJ berkenaan;

(b) Peminjam bertanggungjawab sepenuhnya terhadap keselamatan aset ICT yang dipinjam;

(c) Peminjam hendaklah memulangkan aset ICT yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan;

(d) Peminjam perlu melaporkan secara bertulis dengan segera sekiranya berlaku kerosakan atau kehilangan aset ICT yang dipinjam kepada Ketua PTJ berkenaan;

(e) Aset ICT yang hendak dibawa keluar dari UKM, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan; dan

(a) Sebarang bentuk penyelewengan atau salah guna aset ICT yang dibekalkan oleh UKM hendaklah dilaporkan kepada Ketua PTJ dengan segera.

7.2.3 Pelupusan Aset ICT

Aset ICT yang hendak dilupuskan perlu melalui Prosedur Pelupusan Aset semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat rahsia tidak terlepas kepada pihak tidak bertanggungjawab. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Aset ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; dan

(b) Pelupusan aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa;

7.3 Keselamatan Aset ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Sebarang pertukaran komponen / peralatan dan konfigurasi aset ICT adalah tertakluk kepada kebenaran pihak yang diberi kuasa;

(b) Aset ICT yang hilang/musnah hendaklah dilaporkan kepada Bahagian Keselamatan, Balai Polis/ Balai Bomba dengan segera dan merujuk kepada Prosedur Kehilangan Aset/ Inventori yang berkuatkuasa; dan

(c) Semua baik pulih dan penyelenggaraan aset ICT hendaklah mengikut prosedur ditetapkan.

7.4 Keselamatan Peralatan Mudah Alih (*Mobile Computing)*

Dasar ini memperuntukkan bahawa keselamatan maklumat perlu dipastikan selamat semasa menggunakan peralatan mudah alih. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

(b) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, data, pendedahan maklumat dan capaian tidak sah.

7.5 Keselamatan Media

Dasar ini memperuntukkan bahawa aset ICT perlu dilindungi dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal seperti pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan bolehsediaan maklumat yang disimpan dalam media adalah terjamin dan selamat.

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Menyediakan ruang penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

(b) Semua media perlu dikawal dan dilindungi bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; dan

(c) Akses dan pergerakan media hendaklah direkodkan.

7.5.1 Pengendalian Media

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Akses dan pergerakan media storan hendaklah direkodkan;

(b) Menyediakan ruang penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

(c) Mengehadkan akses untuk memasuki kawasan penyimpanan media, menentukan capaian dan pengedaran kepada personel yang dibenarkan sahaja;

(d) Media yang mengandungi maklumat sensitif perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan. **(A 10**

(e) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;

(f) Semua media *back up* (data / sistem) adalah sulit dan disimpan di tempat yang selamat; dan

(g) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan.

7.5.2 Penghantaran dan Pemindahan Media

Penghantaran atau pemindahan media ke luar PTJ hendaklah mendapat kebenaran daripada Ketua PTJ terlebih dahulu bagi melindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar.

7.5.3 Pelupusan Media

Prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

(a) Proses pelupusan media hendaklah merujuk kepada tatacara pelupusan Universiti dan mendapatkan kelulusan daripada pemilik maklumat terlebih dahulu sebelum maklumat atau kandungan media dihapuskan; dan

(b) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

7.6 Keselamatan Perisian dan Sistem Aplikasi

Dasar ini memperuntukkan bahawa sistem aplikasi adalah termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan perisian. Sistem aplikasi yang dibangunkan perlu mempunyai ciri-ciri keselamatan ICT. Kaedah keselamatan yang bersesuaian perlu dikenalpasti, dirancang dan dilaksanakan semasa proses perolehan, pembangunan dan penyelenggaraan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pengoperasian dan ketepatan maklumat;

(b) perisian untuk kegunaan UKM hendaklah versi terkini dan perlesenan akademik seperti *academic edition* (AE), *academic license* atau *education edition;*

(c) Lesen perisian (*registration code, serials, CD-keys)* perlu disimpan secara berasingan daripada CD atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak;

(d) Pembangunan dan penambahbaikan ke atas sistem aplikasi hendaklah dikawal, dipantau, direkodkan dan disahkan sebelum diguna pakai;

(e) Memastikan sistem aplikasi diuji supaya selamat daripada ancaman;

(f) Ujian keselamatan hendaklah dijalankan ke atas input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan output untuk memastikan data yang telah diproses adalah tepat;

(g) Menghalang sebarang peluang untuk membocorkan atau memanipulasi maklumat;

(h) *Source code* sistem aplikasi (dibangunkan secara dalaman atau luaran) hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan

(i) Sistem aplikasi tidak dibenarkan didemonstrasi kecuali dengan kebenaran.

7.7 Keselamatan Maklumat

7.7.1 Pengendalian Maklumat

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

(a) Maklumat perlu diberikan tahap perlindungan yang bersesuaian. Maklumat hendaklah dikelaskan berdasarkan kepada peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan: Keselamatan Dokumen (Perkara I dan II) seperti berikut:

i. Rahsia Besar;

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

(b) Pengendalian rekod dan maklumat dilaksanakan berdasarkan kepada Arahan Keselamatan: Keselamatan Dokumen (Perkara III dan IV) dan prosedur yang ditetapkan;

(c) Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Menentukan maklumat sedia untuk digunakan;

iii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

iv. Menjaga kerahsiaan katalaluan;

v. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;

vi. Dasar, prosedur dan kawalan penyimpanan maklumat perlu diwujudkan untuk melindungi penyimpanan dan pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

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

viii. Kakitangan bertanggungjawab membuat *back up* maklumat / data rasmi dalam peralatan ICT di bawah kawalannya mengikut keperluan.

(d) Memastikan amalan *clear desk* dan *clear screen* dilaksanakan apabila meninggalkan komputer:

i. menggunakan kemudahan *screen saver; atau*
ii. *logout* daripada sistem aplikasi*;* atau
iii. lain-lain kawalan bersesuaian

7.7.2 Maklumat Dalam E-mel

Dasar ini memperuntukkan bahawa maklumat yang terdapat dalam e-mel perlu dilindungi bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Kemudahan e-mel disediakan untuk warga Universiti, PTJ atau persatuan rasmi Universiti;

(b) Warga Universiti dinasihatkan tidak membuka e-mel daripada penghantar yang tidak diketahui atau diragui dan hendaklah dihapuskan; dan

(c) Warga Universiti hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

7.7.3 Integriti Data

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Urusetia Sistem Aplikasi hendaklah mengambil langkah yang munasabah untuk memastikan bahawa data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini dengan mengambil kira maksud, termasuk apa-apa maksud yang berhubungan secara langsung, yang baginya data peribadi itu dikumpulkan dan diproses selanjutnya; dan

(b) Urusetia Sistem Aplikasi perlu memastikan data peribadi yang dikumpul adalah tepat, lengkap, tidak mengelirukan dan terkini dan digunakan hanya untuk tujuan yang dibenarkan sahaja.

8. KESELAMATAN OPERASI ICT

8.1 Keselamatan Operasi ICT

Operasi ICT perlu berfungsi dengan baik dan selamat daripada sebarang ancaman dan gangguan.

8.1.1 Prosedur Operasi ICT

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Semua prosedur operasi ICT hendaklah dikenalpasti, didokumenkan dengan jelas, dikemaskini dan boleh diguna pakai oleh kakitangan Universiti mengikut keperluan;

(b) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat perlu direkodkan dan dikawal; dan

(c) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan supaya aktiviti pembangunan dan pengujian tidak mengganggu persekitaran operasi.

8.1.2 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Pengubahsuaian yang melibatkan peralatan, sistem dan kemudahan pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pengurusan PTJ terlebih dahulu;

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

(c) Pengemaskinian sistem hanya boleh dilakukan oleh Pentadbir Server berdasarkan prosedur yang telah ditetapkan;

(d) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;

(e) Semua aktiviti perubahan atau pengubahsuaian sistem dan kemudahan pemprosesan maklumat hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat;

(f) Sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;

(g) Data ujian perlu dipilih, dilindungi dan dikawal;

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

(i) Kriteria penerimaan untuk sistem aplikasi baru, peningkatan dan versi baru perlu ditetapkan dan diuji semasa pembangunan dan sebelum penerimaan sistem; dan

(j) Versi baru perisian aplikasi dikeluarkan mengikut keperluan bagi mengatasi masalah pepijat dan ancaman serta meningkatkan fungsinya. Universiti bertanggungjawab mengawal versi perisian aplikasi apabila perubahan atau peningkatan dibuat.

8.1.3 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan

(b) Peralatan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari peralatan yang digunakan sebagai *production*.

8.2 Perlindungan daripada *Malware*

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), dan mengikut prosedur penggunaan yang betul dan selamat;

(b) Memasang dan menggunakan hanya perisian yang berdaftar, berlesen atau tulen sahaja;

(c) Mengimbas semua perisian atau sistem dengan anti virus sebelum membuat instalasi;

(d) Mengemas kini *patches* mengikut keperluan;

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(f) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

(g) Memastikan perisian percuma (*freeware* dan *shareware)* perlu di *uninstall* selepas tamat tempoh penggunaan;

(h) Mengambil langkah pencegahan atau pemulihan serangan kod jahat seperti berikut:
- mengimbas dan menghapus kod jahat menggunakan perisian anti virus yang diluluskan;
- menyemak status proses imbasan dalam laporan log; dan
- tidak melaksanakan *(run)* atau membuka *attachment* daripada *e-mail* yang meragukan.

(i) Melaksanakan jaminan kualiti ke atas semua perisian yang dibangunkan; dan

(j) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya.

8.3 Operasi Rangkaian

Dasar ini memperuntukkan bahawa infrastruktur rangkaian mestilah dikawal dan diuruskan bagi melindungi ancaman kepada sistem aplikasi dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Prosedur dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem rangkaian Universiti;

(b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar;

(c) Kerja-kerja operasi rangkaian (VLAN berbeza) hendaklah diasingkan untuk mengelakkan capaian dan pengubahsuaian yang tidak dibenarkan;

(d) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko (contoh: bencana alam);

(e) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada personel yang dibenarkan sahaja;

(f) Reka bentuk peralatan keselamatan rangkaian (*network security appliance)* hendaklah mengambilkira perkara berikut:
- keperluan pemantauan log;
- kebolehsediaan;
- kerahsiaan; dan
- melindungi maklumat Universiti

(g) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Universiti hendaklah mendapat kebenaran Universiti.

8.4 Pemantauan Aktiviti Pemprosesan Maklumat

Dasar ini memperuntukkan bahawa pemantauan dilakukan untuk mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Log Audit yang merekodkan semua aktiviti perlu diaktifkan dan disimpan untuk tempoh masa yang ditetapkan bagi membantu siasatan dan memantau kawalan capaian;

(b) Prosedur kerja untuk memantau penggunaan kemudahan memproses maklumat diwujudkan;

(c) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

(d) Kesilapan (*fault*) yang dilakukan perlu di log (rekod), di analisa dan di ambil tindakan sewajarnya;

(e) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; dan

(f) Zon masa sistem pemprosesan maklumat perlu diselaraskan dengan satu sumber tepat untuk memastikan semua sistem dalam zon masa yang sama.

Kawalan teknikal keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;

(b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan

(c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

8.5 *Back up*

Bagi memastikan kesinambungan operasi ICT dapat dipulihkan semula setelah berlakunya bencana, *back up* (sistem aplikasi, pangkalan data, rangkaian) hendaklah dilakukan secara berkala atau setiap kali berlaku perubahan. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Mendokumenkan prosedur *back up* dan *restore*;

(b) Media *back up* perlu disimpan di tempat berasingan dan selamat. Akses kepada lokasi storan hendaklah dikawal dengan ketat daripada akses tanpa izin; dan

(c) Menguji media *back up* berdasarkan prosedur yang ditetapkan.

9. KAWALAN CAPAIAN

9.1 Dasar Kawalan Capaian

Dasar ini memperuntukkan bahawa peraturan kawalan capaian hendaklah mengambil kira faktor had capaian dan hak capaian (*authorization)* ke atas maklumat / data dan proses capaian maklumat. Peraturan kawalan capaian dibangunkan dan dikaji semula berdasarkan keperluan perkhidmatan dan keselamatan Universiti.

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Kawalan capaian ke atas aset ICT hendaklah dilaksanakan secara berkesan mengikut keperluan keselamatan dan peranan pengguna;

(b) Kawalan capaian ke atas perkhidmatan rangkaian (dalaman dan luaran);

(c) Kawalan capaian ke atas proses capaian maklumat ; dan

(d) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih.

9.2 Pengurusan Capaian Pengguna

Dasar ini memperuntukkan bahawa prosedur pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan.

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Akaun pengguna yang diwujudkan diberi tahap capaian mengikut peranan dan tanggungjawab pengguna;

(b) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

(c) Pentadbir Sistem boleh menamatkan akaun pengguna atas sebab-sebab berikut:
   i. Bertukar bidang tugas / jabatan;
   ii. Tamat perkhidmatan;
   iii. Tamat pengajian; atau
   iv. Memenuhi kriteria penamatan yang ditetapkan oleh qsistem aplikasi.

(d) Aktiviti capaian oleh pengguna hendaklah direkod, diselenggara dengan sistematik dan dipantau; dan

(e) Penetapan dan penggunaan ke atas hak / had capaian perlu diberi kawalan berdasarkan keperluan skop tugas.

9.2.1 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi pengguna mencapai maklumat dan data dalam sistem aplikasi mestilah mematuhi perkara berikut:

(a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi;

(b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan;

(c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan digalakkan gabungan huruf, angka atau simbol; dan

(d) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;

9.3 Kawalan Capaian Rangkaian

Dasar ini memperuntukkan bahawa capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian perlu dihalang.

9.3.1 Capaian Intranet

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memastikan pengguna yang disahkan sahaja dibenarkan membuat capaian ke rangkaian UKM;

(b) Memastikan s*erver* yang digunakan untuk tujuan penyelidikan yang menggunakan rangkaian secara intensif *(high bandwidth usage)* perlu ditempatkan dalam rangkaian persendirian (LAN) yang dipisahkan daripada rangkaian UKM. Sebarang ujian yang memerlukan penggunaan rangkaian UKM secara terus perlu mendapat kelulusan PTM;

(c) Mewujudkan kaedah pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh *(remote user);*

(d) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;

(e) Mengasingkan capaian mengikut kumpulan pengguna, lokasi dan sistem maklumat dalam rangkaian; dan

(f) Mewujud dan melaksana kawalan laluan *(routing control).*

9.3.2 Capaian Internet

Perkara-perkara berikut perlu dipatuhi:

(a) Penggunaan Internet hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini perlu untuk melindungi daripada kemasukan *malicious code, virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Universiti;

(b) *Content Filtering* digunakan bagi mengawal akses Internet;

(c) Penggunaan *packet shaper* untuk mengawal aktiviti *(video conferencing, video streaming, downloading)* adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan;

Pengguna perlu mematuhi perkara-perkara berikut:

(a) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

(b) Penyambungan capaian ke Internet tanpa kebenaran tidak dibenarkan sama sekali;

(c) Ketua PTJ atau persatuan atau kakitangan Universiti adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan keselamatan laman web masing-masing. Universiti tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan. Universiti juga boleh mengehadkan atau memansuhkan akses kepada tapak laman web tersebut;

(d) Kandungan laman web hendaklah tidak mengandungi maklumat atau terdedah kepada kemasukan maklumat yang menyalahi peraturan Universiti dan undang-undang negara. Ini termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian;

(e) Tidak memuat naik, memuat turun, menyimpan dan menggunakan perisian seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet;

(f) Tidak menyedia, memuat naik, memuat turun dan menyimpan maklumat yang berbentuk keganasan, lucah, hasutan, perkauman dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan sama sekali, kecuali mendapat kebenaran Universiti setelah mendapat sokongan Ketua PTJ bagi tujuan akademik, penyelidikan atau pentadbiran;

(g) Capaian laman yang berbentuk hiburan tidak dibenarkan di waktu pejabat, termasuk tetapi tidak terhad kepada laman *radio online* dan *video streaming* yang membebankan rangkaian Universiti; dan

(h) Universiti berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai.

9.4 Kawalan Capaian Sistem Pengoperasian

Dasar ini memperuntukkan bahawa capaian ke atas sistem operasi perlu dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Mengawal capaian ke atas sistem operasi menggunakan prosedur pengurusan kawalan capaian yang selamat;

(b) Prosedur pengurusan kawalan capaian *server* yang selamat perlulah:

i. Menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat; dan

ii. Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan.

9.5 Kawalan Capaian Sistem Aplikasi

Dasar ini memperuntukkan bahawa kawalan capaian sistem aplikasi bertujuan melindungi sistem aplikasi dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Pengguna hanya boleh menggunakan sistem aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;

(b) Capaian sistem aplikasi melalui jarak jauh (*remote*) terhad kepada perkhidmatan yang dibenarkan sahaja; dan

(c) Sistem aplikasi yang sensitif perlu persekitaran pengkomputeran yang khusus dan terasing.

10. PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN MAKLUMAT

Insiden Keselamatan Maklumat adalah situasi apabila berlakunya pelanggaran Dasar, kegagalan kawalan atau isu keselamatan lain melibatkan sistem dan rangkaian yang boleh menjejaskan operasi perkhidmatan atau mengancam keselamatan maklumat. Oleh itu, ia perlu diurus dengan baik untuk memastikan tindak balas yang dibuat adalah cepat, teratur dan berkesan.

10.1 Melaporkan insiden dan kelemahan keselamatan maklumat

(a) Adalah menjadi tanggungjawab semua pengguna untuk melaporkan insiden keselamatan maklumat dengan kadar segera kepada saluran yang telah ditetapkan; dan

(b) Selain insiden, pengguna dan pembekal perlu melaporkan kelemahan keselamatan maklumat yang ditemui semasa menggunakan sistem dan perkhidmatan.

10.2 Mengendalikan Insiden Keselamatan Maklumat

(a) Laporan yang diterima perlu dinilai dan dipastikan kesahihannya sebelum diklasifikasikan sebagai insiden;

(b) Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenalpasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Universiti;

(c) Bukti insiden keselamatan ICT hendaklah disimpan dan diselenggara. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

i. Mewujud dan mendokumenkan Prosedur Pengurusan Insiden;

ii. Mengenal pasti semua jenis insiden keselamatan maklumat seperti gangguan perkhidmatan yang disengajakan, dan pengubahsuaian perisian tanpa kebenaran;

iii. Menyimpan jejak audit dan melindungi integriti semua bahan bukti; dan

iv. Memaklumkan atau mendapatkan nasihat pihak berkaitan sekiranya perlu.

11. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN ICT

11.1 Pelan Kesinambungan Perkhidmatan ICT

Pelan Kesinambungan Perkhidmatan dibangunkan untuk menentukan pendekatan yang menyeluruh

diambil bagi mengekalkan kesinambungan perkhidmatan ICT. Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan Universiti.

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

(b) Mendokumentasikan dan melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang ditetapkan;

(c) Mengadakan program latihan dan ujian simulasi kepada pengguna mengenai prosedur kecemasan;

(d) Memastikan Pusat Pemulihan Bencana *(Disaster Recovery Centre)* berada dalam keadaan tersedia; dan

(e) Pelan Kesinambungan Perkhidmatan hendaklah diuji secara berkala atau apabila terdapat perubahan persekitaran atau fungsi perkhidmatan untuk memastikan ia sentiasa kekal berkesan.

12. PEMATUHAN

12.1 Pematuhan dan Keperluan Perundangan

12.1.1 Pematuhan Dasar

Setiap warga Universiti hendaklah membaca, memahami dan mematuhi Dasar ini, undang-undang atau peraturan-peraturan yang berkuatkuasa. Semua aset ICT termasuk maklumat yang disimpan di dalamnya adalah hak milik Universiti. Naib Canselor / pegawai yang diberi kuasa berhak untuk memantau sebarang penyalahgunaan sumber ICT Universiti.

12.1.2 Pematuhan Terhadap Keperluan Audit

Pematuhan terhadap keperluan audit adalah perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.

Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem maklumat perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

12.1.3 Keperluan Perundangan

Jika terdapat mana-mana peruntukan di dalam Dasar ini atau sebahagian daripadanya yang diputuskan sebagai tidak sah atau terbatal atau tidak boleh dikuatkuasakan oleh mana-mana peruntukan undang-undang yang sedang berkuatkuasa atau oleh Mahkamah, maka peruntukan tersebut akan menjadi tidak sah atau terbatal dan atau tidak boleh dikuatkuasakan setakat mana yang bertentangan dan akan ditafsirkan seolah-olah peruntukan tersebut tidak menjadi sebahagian daripada Dasar ini.

12.2 Pelanggaran Dasar

(a) Pelanggaran dasar ini boleh mengakibatkan tindakan undang-undang diambil terhadap pengguna;

(b) Pelanggaran dasar ini boleh mengakibatkan tindakan tatatertib diambil terhadap kakitangan dan pelajar. Mereka boleh dihalang atau digantung daripada menggunakan atau mendapatkan kemudahan ICT yang disediakan;

(c) Pelajar yang melanggar dasar ini boleh dikenakan tindakan tatatertib di bawah Kaedah-kaedah UKM (Tatatertib Pelajar-pelajar)1999 [P.U.(A)209/1999];

(d) Kakitangan berstatus tetap Universiti boleh dikenakan tindakan tatatertib di bawah Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605) atau mana-mana peruntukan undang-undang yang berkaitan:

i. Perlembagaan UKM Tahun 2009 S.6 dan S.12
ii. Akta Rahsia Rasmi 1972 (Akta 88) S.8
iii. Akta Komunikasi dan Multimedia 1998 (Akta 588)
iv. Akta Jenayah Komputer 1997 (Akta 563)
v. Akta Pelindungan Data Peribadi 2010 (Akta 709)
vi. Akta Pelindungan Pemberi Maklumat 2010 (Akta 711)

(e) Kakitangan berstatus kontrak, sementara dan sambilan pula boleh dikenakan tindakan sewajarnya termasuklah ditamatkan perkhidmatan.

LAMPIRAN

Senarai Akta / Peraturan Berkaitan

Akta		
Bil.	**Dokumen**	**Nama Dokumen**
1.	Akta 30	Akta Universiti dan Kolej Universiti 1971 Pindaan 2009 [A1342]
2.	Akta 680	Akta Aktiviti Kerajaan Elektronik 2007
3.	Akta 562	Akta Tandatangan Digital 1997
4.	Akta 332	Akta Hakcipta (Pindaan) 1997
5.	Akta 563	Akta Jenayah Komputer 1997
6.	Akta 588	Akta Komunikasi dan Multimedia 1998
7.	Akta 88	Akta Rahsia Rasmi 1972
8.	Akta 709	Akta Perlindungan Data Peribadi 2010
9.	Akta 711	Akta Perlindungan Pemberi Maklumat 2010
10.		Arahan Keselamatan

Pekeliling Am		
Bil.	**Dokumen**	**Nama Dokumen**
11.	Pekeliling Am Bil.1 Tahun 2001	Mekanisme Pelaporan Insiden Keselamatan ICT (ICT)
12.	Pekeliling Am Bil. 3 Tahun 2000	Dasar Keselamatan ICT Kerajaan

Surat Pekeliling Am		
Bil.	**Dokumen**	**Nama Dokumen**
13.	Surat Pekeliling Am Bil.1 Tahun 2008	Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan
14.	Surat Pekeliling Am Bil.6 Tahun 2005	Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam

Pekeliling Kemajuan Pentadbiran Awam		
Bil.	**Dokumen**	**Nama Dokumen**
15.	Pekeliling Kemajuan Perkhidmatan Awam Bil.1 Tahun 2003	Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan

16.	Pekeliling Perbendaharaan	
17.	Perintah-perintah Am	
18.	Pekeliling Bendahari UKM	

Universiti Kebangsaan Malaysia
The National University of Malaysia

UNIVERSITI KEBANGSAAN MALAYSIA,
43600 UKM BANGI,
SELANGOR DARUL EHSAN

w w w . u k m . m y