VERSI 1.7

UTeM

اونيۏرسيتي تيکنيکل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DASAR
KESELAMATAN ICT
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

PPPK | Pusat Perkhidmatan Pengetahuan & Komunikasi

ISI KANDUNGAN

REKOD PINDAAN DOKUMEN

Bil	Tarikh	No. Keluaran / Pindaan	Bab / Muka Surat	Keterangan Pindaan
1.	12 Jun 2015	Versi 1.1	m/s 13, 17 dan 18	Kemaskini nama Pusat Komputer kepada Pusat Pekrhidmatan Pengetahuan dan Komunikasi (PPPK)
			m/s 14	Pertukaran ICTSO daripada Ketua Bahagian Keselamatan ICT dan Datacenter kepada Timbalan Pengarah Infrastruktur
			m/s 15	Pertambahan pentadbir sistem iaitu Ketua Bahagian Pengurusan Data
2.	28 Mei 2016	Versi 1.2	m/s 14	Perubahan pernyataan bagi maksud ICTSO
			m/s 17	Perubahan keanggotaan bagi JKICT UTeM
3.	22 Jun 2017	Versi 1.3	m/s 10	Pertukaran pernyataan perlaksanaan dasar kepada Ketua Pegawai Maklumat (CIO)
			m/s 15	Perubahan Pentadbir Sistem ICT
			m/s 17	Perubahan keanggotaan dan bidang kuasa bagi JKICT UTeM
			m/s 18	Perubahan Pasukan Tindakbalas Insiden Keselamatan ICT UTeM (UTeMCERT)
4.	12 Jun 2018	Versi 1.4	m/s 10, m/s 17	Pertukaran nama jawatan “Ketua Bahagian Dasar dan Latihan”
5.	16 Oktober 2019	Versi 1.5	m/s 54	Perubahan pengurusan kata laluan
			m/s 61	Tambahan klausa bagi kerja jarak jauh

6.	12 Ogos 2020	Versi 1.6	m/s 10	Perubahan keanggotaan dalam Pelaksanaan Dasar
			m/s 15 dan 16	Perubahan Pentadbir Sistem bagi UTeM
			m/s 17	Perubahan keanggotaan bagi JKICT UTeM
			m/s 18	Perubahan keanggotaan bagi UTeMCERT
			m/s 74	Perubahan penyataan Pelanggaran Dasar
			Keseluruhan Helaian	Perubahan Versi
7.	30 April 2021	Versi 1.7	m/s 14	Perubahan Peranan dan tanggungjawab ICTSO
			m/s 71	Tambahan tajuk Pelan Kesinambungan Perkhidmatan kepada Pelan Kesinambungan Perkhidmatan ICT

BAB 8: DASAR KESELAMATAN ICT

0801 Pengenalan

Dasar Keselamatan ICT UTeM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) UTeM (termasuk Jabatan di bawahnya). Dasar ini juga menerangkan kepada semua pengguna di UTeM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UTeM. Dasar ini dibuat berasaskan kepada Dasar Keselamatan ICT MAMPU yang sedia ada.

0802 Objektif

Dasar Keselamatan ICT UTeM diwujudkan untuk menjamin kesinambungan urusan UTeM dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi UTeM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Objektif utama Keselamatan ICT UTeM ialah seperti berikut:

(a) Memastikan kelancaran operasi UTeM dan meminimumkan kerosakan atau kemusnahan;

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

(c) Mencegah salah guna atau kecurian aset ICT UTeM.

0803 Pernyataan Dasar

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT UTeM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

0804 Skop

Aset ICT UTeM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT UTeM menetapkan keperluan-keperluan asas berikut:

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT UTeM ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan UTeM. Contoh komputer, *server*, peralatan komunikasi dan sebagainya;

(b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada UTeM;

(c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

(i) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

(ii) Sistem halangan akses seperti sistem kad akses; dan

(iii) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif UTeM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod UTeM, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

(e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian UTeM bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a)-(e) di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

0805 Prinsip-prinsip

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

(a) Akses atas dasar "perlu mengetahui"

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

(i) 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 perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(ii) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(b) Pengasingan

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

(c) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, *server*, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(d) Pematuhan

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

(e) Pemulihan

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

(f) Saling Bergantungan

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

0806 Penilaian Risiko Keselamatan ICT

UTeM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu UTeM perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

UTeM hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat UTeM termasuklah aplikasi, perisian, *server*, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

UTeM bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

UTeM perlu mengenalpasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
(c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
(d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

Bidang 01 Pembangunan Dan Penyelenggaraan Dasar

0101 Dasar Keselamatan ICT

Objektif:

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

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pegawai Maklumat (CIO) selaku Pengerusi Jawatankuasa Keselamatan ICT UTeM (JKICT UTeM). JKICT UTeM ini terdiri daripada Pengarah PPPK, Pegawai Keselamatan ICT (ICTSO), Timbalan Pengarah PPPK, , Ketua Bahagian Keselamatan ICT dan Pusat Data, Wakil Bahagian Pengurusan Akademik, Wakil Bahgian Pengurusan Sumber Manusia, Wakil Pusat Pengurusan Strategik Kualiti dan Risiko serta 2 wakil daripada Fakulti Teknologi Maklumat & Komunikasi (FTMK) UTeM.

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna ICT UTeM termasuk pihak ketiga.

010103 Penyelenggaraan Dasar

Dasar Keselamatan ICT UTeM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial.

Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT UTeM:

(a) Kenal pasti dan tentukan perubahan yang diperlukan;
(b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT UTeM (JKICTUTeM);
(c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICTUTeM; dan
(d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.

010104 Pengecualian Dasar

Dasar Keselamatan ICT UTeM adalah terpakai kepada semua pengguna ICT UTeM termasuk pihak ketiga dan tiada pengecualian diberikan.

Bidang 02 Organisasi Keselamatan

0201 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT UTeM.

020101 Naib Canselor UTeM

Naib Canselor UTeM adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:

(a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT UTeM;
(b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT UTeM;
(c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan
(d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT UTeM; dan

020102 Pengarah Pusat Perkhidmatan Pengetahuan Dan Komunikasi UTeM

Peranan dan tanggungjawab Pengarah, Pusat Perkhidmatan Pengetahuan Dan Komunikasi (PPPK) UTeM adalah seperti berikut:

(a) Menyediakan Pelan Strategik ICT UTeM bagi merancang penggunaan ICT dalam menyokong pencapaian visi dan misi UTeM;

(b) Memantap dan menyepadukan proses-proses yang *cross-functional* antara PTj bagi menghasilkan sistem penyampaian perkhidmatan yang lebih cekap dan berkesan;

(c) Membangun, mengendali dan mengurus sistem dan infrastruktur ICT yang lebih kukuh dan selamat serta berdasarkan kepada ciri *modular, connectivity, inter-operability* dan *portability;*

(d) Menentukan halatuju sistem aplikasi UTeM bagi mengurangkan masa dan kos pembangunan, pengoperasian dan penyelenggaraan;

(e) Memelihara integriti maklumat, menggalak perkongsian maklumat dan menyediakan mekanisme penyebaran maklumat menerusi ICT kepada pengguna-pengguna yang sah di dalam atau luar UTeM;

(f) Menganggotai jawatankuasa utama yang menggubal dasar dan strategi serta bertanggungjawab terus kepada Naib Canselor; dan

(g) Mempromosikan penggunaan ICT yang berkesan bagi mencapai matlamat strategik UTeM dan bertindak sebagai agen perubahan dan transformasi.

020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi UTeM merupakan pegawai yang dilantik oleh CIO.

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

(a) Mengurus keseluruhan program-program keselamatan ICT UTeM;

(b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT UTeM;

(c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT UTeM kepada semua pengguna;

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

(e) Menjalankan pengurusan risiko;

(f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan UTeM berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

(g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

(h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

(i) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;

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

020104 Pengurus ICT

Pengurus-pengurus ICT bagi UTeM adalah:

(a) Ketua Bahagian Keselamatan ICT dan Pusat Data; dan

(b) Ketua Bahagian Rangkaian.

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

(a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan UTeM;

(b) Menentukan kawalan akses pengguna terhadap aset ICT UTeM;

(c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan

(d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT UTeM.

020105 Pentadbir Sistem ICT

Pentadbir-pentadbir Sistem ICT bagi UTeM adalah:

(a) Ketua Unit Sistem Maklumat Pelajar

b) Ketua Unit Sistem Maklumat Kewangan Bersepadu

c) Ketua unit Sistem Maklumat Sumber Manusia

(d) Ketua Unit Sistem Maklumat Pasca Siswazah

(e) Ketua Unit Sistem Maklumat URIS dan Sistem Maklumat Fasiliti

(f) Ketua Unit Sistem Maklumat Kenderaan Universiti

(g) Ketua Unit Aplikasi Sokongan

(h) Ketua Unit Sistem Hal Ehwal Pelajar

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

(a) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sistem sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT UTeM;
(b) Memantau aktiviti capaian sistem aplikasi pengguna;
(c) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;
(d) Menganalisa dan menyimpan rekod jejak audit; dan
(e) Menyediakan laporan mengenai aktiviti capaian mengikut keperluan.

020106 Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

(a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT UTeM;
(b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
(c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
(d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT UTeM dan menjaga kerahsiaan maklumat UTeM;
(e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan
(f) Menghadiri program-program kesedaran mengenai keselamatan ICT.

020107 Jawatan Kuasa Keselamatan ICT UTeM

Jawatankuasa Keselamatan ICT UTeM (JKICTUTeM) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT UTeM.

Keanggotaan JKICT UTeM adalah seperti berikut:

Pengerusi: Ketua Pegawai Maklumat (CIO)

Timbalan Pengerusi: Timbalan Ketua Pegawai Maklumat

Ahli:

(a) Pengarah, Pusat Perkhidmatan Pengetahuan Dan Komunikasi (PPPK)

(b) Timbalan Pengarah Infrastruktur ICT;

(c) Timbalan Pengarah Infostruktur ICT;

(d) Ketua Bahagian Keselamatan ICT dan Pusat Data;

(e) Seorang wakil Bahagian Pengurusan Akademik (BPA), seorang wakil Bahagian Pengurusan Sumber Manusia (BPSM), Seorang wakil Pusat Pengurusan Strategik Kualiti dan Risiko (PPSKR) serta 2 orang wakil daripada Fakulti Teknologi Maklumat & Komunikasi (FTMK) UTeM (lantikan dari masa ke semasa)

Bidang kuasa:

(a) Memperakukan/meluluskan dokumen DKICT UTeM;

(b) Memantau tahap pematuhan keselamatan ICT;

(c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam UTeM yang mematuhi keperluan DKICT UTeM;

(d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

(e) Memastikan DKICT UTeM selaras dengan dasar-dasar ICT kerajaan semasa;

(f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;

(g) Membincang tindakan yang melibatkan pelanggaran DKICT UTeM; dan

(h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.

020108 Pasukan Tindak Balas Insiden Keselamatan ICT UTeM (UTeMCERT)

Keanggotaan UTeMCERT adalah seperti berikut:

Pengarah UTeMCERT : Timbalan Pengarah Infrastruktur ICT

Pengurus UTeMCERT : Ketua Bahagian Keselamatan ICT dan Pusat Data

Ahli :

(a) Timbalan Pengarah Infostruktur

(b) Ketua Bahagian Rangkaian;

(a) Ketua Bahagian Pengurusan Pengetahuan;

(c) Ketua Unit Keselamatan ICT dan Unit Pematuhan & Pengendalian Insiden;

(d) Ketua Unit Pusat Data dan Unit Pangkalan Data;

(e) Ketua Unit Rangkaian dan Aplikasi Rangkaian;

(f) Tiga orang wakil daripada Fakulti Teknologi Maklumat dan Komunikasi (FTMK) UTeM.

Peranan dan tanggungjawab UTeMCERT adalah seperti berikut:

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

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

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

(d) Menasihati JKICT UTeM berkaitan tindakan pemulihan dan pengukuhan;

(e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada UTeM.

0202 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.

Perkara yang perlu dipatuhi termasuk yang berikut:

(a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT UTeM;

(b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

(c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;

(d) Akses kepada aset ICT UTeM perlu berlandaskan kepada perjanjian kontrak;

(e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

   (i) Dasar Keselamatan ICT UTeM;

   (ii) Tapisan Keselamatan;

   (iii) Perakuan Akta Rahsia Rasmi 1972; dan

   (iv) Hak Harta Intelek.

Bidang 03 Pengurusan Aset

0301 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan keselamatan yang bersesuaian ke atas semua aset ICT UTeM.

030101 Inventori Aset

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta dan inventori dan sentiasa dikemas kini;

(b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

(c) Mengenalpasti lokasi semua aset ICT yang telah ditempatkan di UTeM;

(d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan

(e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

0302 Pengelasan dan Pengendalian Maklumat

Objektif

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

030201 Pengelasan Maklumat

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

(a) Rahsia Besar;

(b) Rahsia;

(c) Sulit; atau

(d) Terhad.

030202 Pengendalian Maklumat

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

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, pengantaran, penyampaian, pertukaran dan pemusnahan; dan

(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

Bidang 04 Keselamatan Sumber Manusia

Objektif

Memastikan semua sumber manusia yang terlibat termasuk staf UTeM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua yang terlibat hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

040101 Sebelum Perkhidmatan

Memastikan semua sumber manusia yang terlibat termasuk staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT.

Perkara yang mesti dipatuhi termasuk yang berikut:

(a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan;

(b) Menjalankan tapisan keselamatan untuk staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan

(c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

040102 Dalam Perkhidmatan

Memastikan semua sumber manusia yang terlibat termasuk staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT.

Perkara yang mesti dipatuhi termasuk yang berikut:

(a) Memastikan staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan UTeM;

(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada staf UTeM, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa;

(c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas staf UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan UTeM; dan

(d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.

040103 Bertukar Atau Tamat Perkhidmatan

Memastikan semua staf UTeM yang tamat perkhidmatan / belajar atau bertukar dari UTeM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur.

Perkara yang perlu dipatuhi termasuk:

(a) Memastikan semua aset ICT dikembalikan kepada PTj mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

(b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan UTeM dan/atau terma perkhidmatan.

Bidang 05 Keselamatan Fizikal Dan Persekitaran

0501 Keselamatan Kawasan

Objektif:

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

050101 Kawalan Kawasan

Kawasan larangan lokasi ICT bagi UTeM ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga UTeM yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam.

Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:

(a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran;

(b) Akses adalah terhad kepada warga UTeM yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

(c) Pemantauan dibuat menggunakan Access Door melalui Kad Staf atau lain-lain peralatan yang sesuai;

(d) Peralatan Access Door dan Log akses perlu diperiksa secara berjadual;

(e) Pelawat yang keluar masuk ke kawasan larangan perlu mendapat keizinan dan diawasi oleh pegawai yang bertanggungjawab;

(f) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam;

(g) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;

(h) Memperkukuh dinding dan siling;

(i) Menghadkan jalan keluar masuk;

(j) Mengadakan kaunter kawalan; dan

(k) Menyediakan tempat atau bilik khas untuk pelawat.

050102 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

(a) Warga UTeM

(i) Semua warga UTeM hendaklah memakai atau mengenakan kad ID UTeM sepanjang waktu bertugas; dan

(ii) Semua kad ID UTeM hendaklah diserahkan kembali kepada UTeM apabila pengguna berhenti atau bersara.

(b) Pelawat

(i) Setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan pas ini hendaklah dikembalikan semula selepas tamat lawatan.

(c) Kehilangan pas mestilah dilaporkan dengan segera.

050103 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada warga UTeM yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan ICT di UTeM adalah Datacenter, bilik server, bilik comrack, bilik operasi rangkaian dan lain-lain kawasan yang diwartakan sebagai kawasan larangan.

(a) Akses kepada kawasan larangan hanyalah kepada warga UTeM yang dibenarkan sahaja;

(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan

(c) Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengarah PPPK atau Ketua Pusat Tanggungjawab.

0502 Keselamatan Peralatan

Objektif:
Melindungi peralatan ICT UTeM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

050201 Peralatan ICT

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran, penambahan, penanggalan atau penggantian perkakasan dan konfigurasi yang telah ditetapkan;

(c) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran PPPK;

(d) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada PPPK untuk dibaik pulih;

(e) Pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh PPPK seperti komputer peribadi, *notebook* dan *server* yang berada di bawah

tanggungjawab mereka sentiasa aktif (*activated*) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan;

(f) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan PPPK;

(g) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salahguna;

(h) Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset;

(i) Jika peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari / kabinet / peti besi / stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT dalam kawalan Pusat Tanggungjawab masing-masing;

(j) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

(k) UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;

(l) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci;

(m) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;

(n) Peralatan ICT yang hendak dibawa keluar dari premis UTeM, perlulah mendapat kelulusan Ketua-ketua Bahagian PPPK yang berkenaan bagi tujuan pemantauan;

(o) Aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut peraturan atau pekeliling terkini Pejabat Bendahari UTeM;

(p) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; dan

(q) Sebarang bentuk penyelewengan atau salah guna infrastruktur ICT hendaklah dilaporkan kepada ICTSO.

050202 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik dan media-media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil:

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

(b) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu;

(c) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;

(d) Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat;

(e) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti (*data safe)* yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;

(f) Storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja;

(g) Akses dan pergerakan media storan perlu direkodkan;

(h) Perkakasan *backup* (*CD/DVD duplicator)* hendaklah diletakkan di tempat yang lebih privasi dan terhad kepada pengguna yang dibenarkan sahaja; dan

(i) Sebarang kehilangan media storan yang berlaku hendaklah dilaporkan kepada PTj masing-masing.

050203 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;

(b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan

(c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

050204 Media Perisian Dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan UTeM;

(b) Sistem aplikasi dalaman tidak dibenarkan dibentangkan atau diagih kepada pihak lain kecuali dengan kebenaran Pengarah PPPK;

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

(d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.

050205 Penyelenggaraan Perkakasan

Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

(a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

(b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

(c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

(d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

(e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

050206 Peralatan di Luar Premis

Perkakasan yang dibawa keluar dari premis UTeM adalah terdedah kepada pelbagai risiko. Perkakasan yang dibawa keluar premis UTeM merangkumi:

(a) Penggunaan perkakasan secara sementara bagi keperluan mesyuarat, latihan dan sebagainya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Peralatan perlu dilindungi dan dikawal sepanjang masa;

(b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian;

(c) Mendapatkan kelulusan mengikut peraturan sedia ada UTeM bagi membawa keluar peralatan tertakluk kepada tujuan yang dibenarkan; dan

(d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.

050207 Pelupusan Perkakasan

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada aset tetap atau inventori yang dibekalkan oleh UTeM dan ditempatkan di UTeM. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan UTeM:

(a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding* atau pembakaran;

(b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

(c) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *disket* atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan;

(d) Peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

(e) Pegawai Pemeriksa Pelupusan hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

(f) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;

(h) Pengguna ICT adalah **DILARANG SAMA SEKAL**I daripada melakukan perkara-perkara seperti berikut:

    (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;

(ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM*, *hardisk*, *motherboard* dan sebagainya;

(iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di UTeM;

(iv) Memindah keluar dari UTeM mana-mana peralatan ICT yang hendak dilupuskan; dan

(v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab UTeM;

(j) Proses pelupusan mestilah mengikut Peraturan atau Pekeliling terkini yang dikeluarkan oleh Pejabat Bendahari UTeM**;** dan

(k) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti Arahan Keselamatan dan tatacara Jabatan Arkib Negara.

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT UTeM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada PPPK.

Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:

(a) Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat (bilik percetakan, peralatan komputer dan sebagainya) dengan teliti;

(b) Semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;

(c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;

(d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT;

(e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;

(f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;

(g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya satu (1) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu;

(h) Mengadakan *preventive maintainance*; dan

(i) Menggunakan vakum yang memenuhi piawai untuk membersihkan peralatan.

050302 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan;

(b) Memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual sekurang-kurangnya satu (1) kali setahun;

(c) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai; dan

(d) Suhu hendaklah terkawal dalam had suhu peralatan rangkaian berkenaan dengan memasang penghawa dingin khusus (*precision aircond*) sepanjang masa.

050303 Kabel

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

(a) Menggunakan kabel mengikut spesifikasi yang telah ditetapkan;

(b) Melindungi kabel di kawasan awam dengan memasang *conduit* atau lain-lain mekanisma perlindungan, untuk mengelak daripada kerosakan yang disengajakan atau tidak disengajakan;

(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*;

(d) Melabelkan kabel menggunakan kod dan label yang mengikut piawaian; dan

(e) Pusat pendawaian/*Network Operating Center* hendaklah sentiasa berkunci dan hanya boleh dicapai oleh staf yang dibenarkan.

050304 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan oleh Pejabat Keselamatan dan Kesihatan Pekerjaan (OSHA) UTeM;

(b) Melaporkan insiden kecemasan kepada Pegawai Keselamatan di Pejabat Keselamatan UTeM;

(c) Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan

(d) Merancang dan mengadakan latihan kebakaran bangunan (*fire drill*) secara berkala.

0504 Keselamatan Dokumen

Objektif:
Melindungi maklumat UTeM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

050401 Dokumen

Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi:

(a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;

(b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;

(c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;

(d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan

(e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.

Bidang 06 Pengurusan Operasi Dan Komunikasi

0601 Pengurusan Prosedur Operasi

Objektif:

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal;

(b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

(c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Ketua Pegawai Tanggungjawab atau pemilik aset ICT terlebih dahulu;

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

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

(d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

060103 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

(b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan

(c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

060201 Perkhidmatan Penyampaian

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

(a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;

(b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau dan disemak dari semasa ke semasa; dan

(c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

0603 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.

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.

060302 Penerimaan Sistem

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

0604 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.

060401 Perlindungan dari Perisian Berbahaya

Perkara-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) serta mengikut prosedur penggunaan yang betul dan selamat;

(b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

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

(d) Mengemaskini anti virus dengan pattern antivirus yang terkini;

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

(f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

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

(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

(i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

060402 Perlindungan dari *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

0605 *Housekeeping*

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

060501 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi secara berjadual;

(b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat;

(c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;

(d) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.

0606 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

(b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

(c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

(d) Semua peralatan mestilah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi;

(e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pengurus ICT;

(f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan UTeM;

(g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

(h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UTeM;

(i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan UTeM adalah tidak dibenarkan;

(k) Semua pengguna hanya dibenarkan menggunakan rangkaian UTeM sahaja dan penggunaan modem adalah dilarang sama sekali; dan

(l) Kemudahan bagi wireless LAN mesti mempunyai kawalan keselamatan

0607 Pengurusan Media

Objektif:

Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

060701 Penghantaran dan Pemindahan

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

060702 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

(a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

(b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

(c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

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

(e) Menyimpan semua media di tempat yang selamat; dan

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

060703 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:

(a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;

(b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan

(c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

0608 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara UTeM dan agensi luar terjamin.

060801 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara UTeM dengan agensi luar;

(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari UTeM; dan

(d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

060802 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di UTeM hendaklah dipantau secara berterusan oleh Pentadbir Sistem ICT untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuat kuasa.

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut :

(a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh UTeM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

(b) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

(c) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

(d) Pengguna dinasihatkan menggunakan lampiran, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

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

(f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

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

(h) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

(i) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

(j) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

(k) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan

(l) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.

0609 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

060901 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:

(a) Sebarang percubaan pencerobohan kepada sistem ICT UTeM;

(b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);

(c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

(d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;

(e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

(f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; dan

(g) Aktiviti penyalahgunaan akaun e-mel.

060902 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut :

(a) Rekod setiap aktiviti transaksi;

(b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

(c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan

(d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara.

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

060903 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut :

(a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

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

(c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT atau Pengurus ICT hendaklah melaporkan kepada ICTSO dan Pengarah PPPK.

060904 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

(b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;

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

(d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

(e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

(f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam UTeM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

Bidang 07 Kawalan Capaian

0701 Dasar Kawalan Capaian

Objektif:

Memahami dan mematuhi keperluan keselamatan dalam membuat capaian dan menggunakan aset ICT UTeM.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

(c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan

(d) Kawalan ke atas kemudahan pemprosesan maklumat.

0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT UTeM.

070201 Akaun Pengguna

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

(a) Akaun yang diperuntukkan oleh UTeM sahaja boleh digunakan;

(b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

(c) Akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;

(d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan UTeM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

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

(f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab- sebab berikut:

  (i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) bulan;

  (ii) Bertukar bidang tugas kerja;

  (iii) Bertukar ke agensi lain;

  (iv) Bersara; atau

  (v) Ditamatkan perkhidmatan.

070202 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

070203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh UTeM seperti berikut:

(a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

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

(c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf besar, huruf kecil, simbol dan nombor;

(d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

(e) Kata laluan windows hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama;

(f) Kata laluan hendaklah **TIDAK** dipaparkan semasa input, dalam laporan atau media lain;

(g) Kuatkuasakan pertukaran kata laluan semasa *log in* kali pertama atau selepas *log in* kali pertama atau selepas kata laluan diset semula;

(h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

(i) Had kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa selama **3 minit** atau setelah diset semula oleh Helpdesk;

(j) Sistem tidak membenarkan penggunaan semula katalaluan semasa bagi kata laluan yang baru selama tiga (3) kitaran yang bersamaan 270 hari dimana setiap satu (1) kitaran untuk sesuatu kata laluan itu tamat tempoh adalah bersamaan setiap 90 hari;

(k) Kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan; dan

(l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

070204 *Clear Desk* dan *Clear Screen*

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-

(a) Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer;

(b) Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan

(c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

0703 Kawalan Capaian Rangkaian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

070301 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

(a) Memastikan pengguna boleh membuat capaian ke atas perkhidmatan yang dibenarkan sahaja;

(b) Menempatkan atau memasang antaramuka yang bersesuaian di antara UTeMnet, rangkaian agensi lain dan rangkaian awam;

(c) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan

(d) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

(e) Mengguna kaedah pengenalan automatik berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian;

(f) Mengawal capaian fizikal dan logikal ke atas kemudahan *port diagnostic* dan konfigurasi jarak jauh;

(g) Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian; dan

(h) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) untuk memastikan pematuhan ke atas peraturan UTeM.

070302 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Penggunaan Internet di UTeM hendaklah dipantau secara berterusan oleh Pengurus ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam UTeMnet;

(b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

(c) Penggunaan proksi yang telah ditetapkan oleh UTeM bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan;

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

(e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

(f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah PPPK yang diberi kuasa;

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

(h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua PTj sebelum dimuat naik ke Internet;

(i) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

(j) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UTeM;

(k) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua PTj terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

(l) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali tanpa kelulusan Pengarah PPPK; dan

(m) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

  (i) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

  (ii) Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

0704 Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

070401 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer.

Kemudahan ini juga perlu bagi:

(a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan;

(b) Merekodkan capaian yang berjaya dan gagal;

(c) Membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan); dan

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

(a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;

(b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian;

(c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem; dan

(d) Menyediakan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

(a) Mengawal capaian ke atas sistem operasi menggunakan prosedur *log in* yang terjamin;

(b) Mewujudkan satu pengenalan diri (*ID*) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna;

(c) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;

(d) Mengawal penggunaan utiliti yang berkeupayaan melepasi sistem dan aplikasi terhad;

(e) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi;

(f) Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan

(g) Menghadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.

070402 Kad ID

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;

(b) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan

(c) Sebarang kehilangan dan kerosakan perlu dilaporkan kepada Pejabat Keselamatan, UTeM.

0705 Kawalan Capaian Aplikasi Dan Maklumat

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

070501 Capaian Aplikasi Dan Maklumat

Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di UTeM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah selamat, langkah-langkah berikut perlu dipatuhi:

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

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

(c) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini;

(d) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;

(e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;

(f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja;

(g) *Session timeout* hendaklah dilaksanakan.

0706 Peralatan Mudah Alih

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh

070601 Peralatan Mudah Alih

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan kehilangan atau pun kerosakan; dan

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

070602 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.

Bidang 08 Perolehan, Pembangunan Dan Penyelenggaraan Sistem

0801 Keselamatan Dalam Membangunkan Dan Menyelenggara Sistem Aplikasi

Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

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

(c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan

(d) Semua sistem yang dibangunkan dan diselenggara sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

080102 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan

(b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

0802 Kawalan Kriptografi

Objektif:
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

080201 Enkripsi

Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

080202 Tandatangan Digital

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

080203 Pengurusan Infrastruktur Kunci Awam (PKI)

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

0803 Keselamatan Fail Sistem

Objektif:

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

080301 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;

(b) Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;

(c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;

(d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan

(e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

(a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai;

(b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga;

(c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;

(d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan

(e) Menghalang sebarang peluang untuk membocorkan maklumat.

080402 Pembangunan Perisian Secara *Outsource*

Pembangunan perisian secara *outsource* perlu diselia dan dipantau sentiasa oleh pemilik sistem. Aspek teknikal perlu dikawalselia oleh PPPK. Klausa mengenai pemindahan teknologi (*Transfer of Technology*) dan penyerahan serta pemilikan *source code* dari pembekal kepada PPPK hendaklah dinyatakan dalam dokumen kontrak. Ini bagi memastikan kerja-kerja penyelenggaraan dapat dikawalselia oleh PPPK. Pihak ketiga perlulah menyediakan dokumentasi manual pengguna dan dokumentasi sistem yang lengkap dan terkini kepada PPPK.

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

080501 Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini 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.

0806 Keselamatan Perisian Sistem Aplikasi

Pengurus ICT atau Pentadbir Sistem ICT adalah bertanggungjawab memastikan Kawalan keselamatan dilaksana bagi mengelak berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. PPPK bertanggungjawab menyediakan kawalan dan kemudahan seperti berikut:

(a) Sistem keselamatan berpusat dengan kawalan capaian penggunaan satu ID dan kata laluan untuk semua aplikasi;
(b) Profil capaian yang menghadkan tahap capaian maklumat serta fungsi berdasarkan peranan pengguna;
(c) Kawalan peringkat sistem aplikasi dengan mengadakan sistem log yang menentukan akauntabiliti kepada semua pengguna; dan

(d) Penetapan pemilik maklumat adalah merujuk kepada pemilik sistem.

0807 Keselamatan Pangkalan Data

Pengurus ICT dan Pentadbir Sistem ICT adalah bertanggungjawab ke atas integriti maklumat yang disimpan dalam pangkalan data kekal dan terjamin. Perkara yang perlu dipatuhi adalah seperti berikut:

(a) Sistem Pengurusan Pangkalan Data memastikan integriti dalam pengemaskinian dan capaian maklumat; dan

(b) Kawalan capaian kepada maklumat ditentukan oleh Pengurus ICT.

0808 Perubahan Versi

Pentadbir Sistem ICT adalah bertanggungjawab mengawal versi sistem aplikasi apabila perubahan atau peningkatan dibuat dan prosedur kawalan perubahan versi perlu sentiasa dipatuhi.

0809 Penyimpanan Kod Sumber (*Source Code*)

Pengurus ICT dan Pentadbir Sistem ICT adalah bertanggungjawab mengurus dan melaksanakan kawalan penyimpanan kod sumber bagi sistem aplikasi yang dibangunkan secara dalaman atau luaran untuk tujuan penyelenggaraan dan peningkatan yang merangkumi:

(a) Mewujudkan prosedur penyelenggaraan versi terkini.

(b) Mendokumenkan prosedur *back up* kod sumber bagi penyelenggaraan versi terkini.

(c) Menyimpan *back up* kod sumber di dua (2) lokasi yang berasingan.

0810 Pengujian Aplikasi

Pentadbir Sistem ICT adalah bertanggungjawab menguji atucara, modul, sistem aplikasi dan integrasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan. Bagi menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya, persekitaran yang berbeza untuk pembangunan sistem dan pengoperasian sistem perlu diwujudkan. Sekiranya persekitaran berasingan untuk pembangunan sistem tidak dapat dilaksanakan, langkah-langkah berikut hendaklah dilakukan:

(a) Menggunakan data ujian (*dummy*) atau data lapuk (*historical*).

(b) Mengawal penggunaan data terpilih (*classified*).

(c) Menghadkan capaian kepada staf yang terlibat sahaja.

(d) Mengadakan kaedah pemberitahuan (*flag system*) sekiranya capaian dan pengemaskinian maklumat dilakukan.

(e) Menghapuskan maklumat yang digunakan selepas selesai pengujian (terutamanya apabila menggunakan data lapuk).

Bidang 09 Pengurusan Pengendalian Insiden Keselamatan

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan bagi memastikan sistem ICT UTeM dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej UTeM dan sistem penyampaian perkhidmatan.

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan UTeMCERT dengan kadar segera:

(a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

(b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

(c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;

(d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

(e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

(f) Prosedur pelaporan insiden keselamatan ICT berdasarkan:

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

  (ii) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

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 mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada UTeM. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan. -

Kawalan-kawalan yang perlu diambilkira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

(a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti;
(b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan ICT;
(d) Menyediakan tindakan pemulihan segera; dan
(e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

Bidang 10 Pengurusan Kesinambungan Perkhidmatan

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

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

100101 Pelan Kesinambungan Perkhidmatan ICT

Pelan Kesinambungan Perkhidmatan ICT (*Business Continuity Management*, *BCM*) 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 JKICTUTeM dan perkara-perkara berikut perlu diberi perhatian:

(a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
(b) Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap operasi UTeM bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;
(c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
(d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;
(e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
(f) Membuat penduaan; dan
(g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

Pelan *BCM* perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

(b) Senarai staf UTeM dan pihak ketiga berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan staf yang tidak dapat hadir untuk menangani insiden;

(c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

(d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

(e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan pelan *BCM* perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan *BCM* hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi operasi UTeM untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan *BCM* hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan staf yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

UTeM hendaklah memastikan salinan pelan *BCM* sentiasa dikemaskini dan dilindungi seperti di lokasi utama.

Bidang 11 Pematuhan

1101 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT UTeM.

110101 Pematuhan Dasar

Setiap pengguna di UTeM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT UTeM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di UTeM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah atau pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT UTeM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber UTeM.

110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.

110103 Pematuhan Keperluan Audit

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

Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi 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.

110104 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT UTeM dan Peraturan serta garis Panduan di bawahnya boleh dikenakan tindakan tatatertib.