CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY (CICT)

UNIVERSITI TEKNOLOGI MALAYSIA (UTM)

DASAR KESELAMATAN ICT (DKICT)
CICT-UTM-ISMS-P1-001

ISO/IEC 27001:2013

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT UTM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) UTM. Dasar ini juga menerangkan kepada semua pengguna di UTM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UTM.

OBJEKTIF

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

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi UTM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT UTM ialah seperti berikut:

a) Memastikan kelancaran operasi UTM 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 UTM.

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 universiti 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 hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT UTM 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 semulajadi 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.

SKOP

Aset ICT UTM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT UTM 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 UTM, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT UTM ini merangkumi perlindungan kepada semua bentuk maklumat universiti 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 UTM. Contoh komputer, pelayan, 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 UTM;

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong asset 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 UTM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod UTM, 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 UTM 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.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT UTM 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;

b) Hak akses minimum

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

c) **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT UTM. 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 standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d) Pengasingan

Tugas mewujud, memadam, mengemas kini, 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;

e) Pengauditan

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

f) Pematuhan

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

g) Pemulihan

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

h) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama

lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

UTM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu, UTM 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.

UTM 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 UTM termasuklah aplikasi, perisian, pelayan, 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.

UTM 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.

UTM perlu mengenal pasti 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;

c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d) Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

BIDANG 01

PEMBANGUNAN DAN PENYENGGARAAN DASAR

Huraian	UTM hendaklah mewujudkan dan menyelenggarakan dasar-dasar yang jelas yang dapat menjamin perlindungan ke atas kerahsiaan, integriti dan ketersediaan maklumat dan seterusnya menjamin kesinambungan urusan serta perkhidmatan dengan meminimumkan kesan insiden Keselamatan ICT.
Objektif	Untuk menentukan hala tuju dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan undang-undang.

0101 Pemakaian Dasar Keselamatan ICT UTM

Dasar Keselamatan ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Universiti Teknologi Malaysia (UTM) dan perundangan yang berkaitan untuk memastikan kelancaran operasi UTM secara berterusan, meminimumkan kerosakan atau kemusnahan aset ICT melalui usaha pencegahan insiden ICT berdasarkan ciri-ciri keselamatan ICT iaitu kerahsian, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.

UTM-010101 Perlaksanaan Dasar	**Tindakan**
Pelaksanaan dasar ini akan dijalankan oleh Naib Canselor UTM selaku Pengerusi Majlis ICT UTM dibantu oleh Timbalan Naib Canselor (Pembangunan) selaku Pengerusi Jawatankuasa Teknikal ICT UTM (JTICT UTM), Ketua Pegawai Maklumat (CIO), Pengarah Pusat Teknologi Maklumat dan Komunikasi (CICT), Pegawai Keselamatan ICT (ICTSO), Timbalan-timbalan Pengarah CICT dan sebahagian Ketua PTJ yang dilantik.	Naib Canselor
UTM-010102 Penyebaran Dasar	**Tindakan**
Dasar ini perlu disebarkan dan adalah terpakai kepada semua pengguna ICT di UTM (termasuk kakitangan, pelajar, pembekal, pakar runding dan sebagainya)	CIO, ICTSO dan HEK

UTM-010103 Penyelenggaraan Dasar	**Tindakan**
Dasar Keselamatan ICT UTM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang perlu dipatuhi berhubung dengan penyelenggaraan Dasar Keselamatan ICT UTM: a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemuka cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Majlis ICT UTM c) Perubahan yang telah dipersetujui oleh Majlis ICT UTM dimaklumkan kepada semua pengguna; dan d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	CIO, ICTSO
UTM-010104 Pengecualian Dasar	**Tindakan**
Dasar Keselamatan ICT UTM adalah terpakai kepada semua pengguna aset ICT UTM dan tiada pengecualian diberikan.	Semua

0102 Semakan Dan Pindaan Dasar

Objektif:

Dasar Keselamatan ICT UTM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

UTM-010201 Prosedur Penyenggaraan Dasar Keselamatan ICT	Tindakan
Prosedur penyelenggaraan Dasar Keselamatan ICT UTM adalah termasuk yang berikut: a) Menyemak dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan perubahan secara bertulis kepada Pusat Teknologi Maklumat dan Komunikasi (CICT), Universiti Teknologi Malaysia dan dibawa ke dalam Mesyuarat Majlis ICT UTM untuk kelulusan; dan c) Memaklumkan perubahan dasar yang telah dipersetujui oleh Pusat Teknologi Maklumat dan Komunikasi (CICT), Universiti Teknologi Malaysia kepada semua pengguna.	Semua

BIDANG 02

PENGURUSAN KESELAMATAN ICT

Huraian	Satu rangka kerja pengurusan keselamatan ICT perlu diwujudkan supaya keselamatan ICT dilaksanakan dengan lebih sistematik, berstruktur, lancar dan berkesan.
Objektif	Untuk menguruskan keselamatan ICT di UTM.

0201 Pengurusan Keselamatan ICT

Objektif:

Pengurusan keselamatan ICT perlu diwujudkan untuk memastikan keselamatan ICT dilaksanakan dengan lebih sistematik, berstruktur, lancar dan berkesan.

0202 Struktur Organisasi

Objektif:

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

UTM-020201 Naib Canselor	**Tindakan**
Peranan dan tanggungjawab Naib Canselor (NC) adalah seperti berikut: a) Memastikan semua pengguna memahami peruntukan- peruntukan di bawah Dasar Keselamatan ICT Universiti; b) Memastikan semua pengguna mematuhi dan tertakluk kepada Dasar Keselamatan ICT Universiti; c) Memastikan semua keperluan organisasi (sumber kewangan, kakitangan dan perlindungan keselamatan)adalah mencukupi;	Naib Canselor

d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Universiti; dan e) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT UTM;	
UTM-020202 Majlis ICT UTM	**Tindakan**
Tugas-tugas Majlis ICT UTM: a) Menetapkan dan memperaku visi, arah tuju dan strategi ICT Universiti; b) Memperaku dan mengesahkan polisi /dasar dan prosedur berkaitan dengan pengurusan dan pentadbiran ICT Universiti; c) Memperakukan pelan strategik ICT Universiti dan memantau pelaksanaannya; d) Menilai pencapaian prestasi ICT Universiti semasa dan; e) Menyelaras dan menyeragamkan pelaksanaan ICT disemua PTJ.	Majlis ICT UTM
UTM-020203 Ketua Pegawai Maklumat (CIO)	**Tindakan**
Ketua Pegawai Maklumat (CIO) bagi UTM ialah Pengarah CICT. Peranan dan tanggungjawab CIO adalah seperti berikut: a) Membantu Naib Canselor dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Mempengerusikan Mesyuarat Jawatankuasa Teknikal ICT (JTICT), UTM. c) Menentukan keperluan keselamatan ICT; d) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT UTM serta pengurusan risiko dan pengauditan; dan e) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT UTM.	CIO
UTM-020204 Pegawai Keselamatan ICT (ICTSO)	**Tindakan**
Pegawai Keselamatan ICT (ICTSO) bagi UTM ialah Ketua Bahagian Keselamatan ICT, Pusat Teknologi Maklumat dan Komunikasi, UTM.	ICTSO

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a) Merancang dan mengurus keseluruhan program-program keselamatan ICT UTM;

b) Melaksanakan Dasar Keselamatan ICT UTM;

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

d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada Pengurus ICT;

e) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT UTM;

f) Melaksanakan pengurusan risiko;

g) Melaksanakan audit, mengkaji semula, merumus tindak balas pengurusan universiti berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

h) Memberi amaran kepada warga kampus UTM terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

i) Menjalankan peranan dan tanggungjawab sebagai Pengurus Pasukan UTMCERT;

j) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) UTM dan memaklumkannya kepada Pengurus ICT dan CIO;

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

l) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT;

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

UTM-020205 Pengurus IT	**Tindakan**
Tugas Pengurus Fasiliti a) Menerima maklumbalas tahap penyampaian perkhidmatan ICT yang disediakan dari setiap PTJ ke arah meningkatkan kualiti perkhidmatan ICT Universiti; b) Memperolehi keperluan ICT di setiap PTJ untuk membantu perancangan ICT Universiti; c) Menangani isu dan cabaran berkaitan perkhidmatan ICT di setiap PTJ. d) Memberi pendedahan dan informasi mengenai perkhidmatan-perkhidmatan baru ICT yang digunapakai di Universiti; dan e) Bertindak sebagai penghubung di antara CICT dan pengguna IT di semua PTJ.	Pengurus Fasiliti
UTM-020206 Pentadbir Sistem ICT	**Tindakan**
Pentadbir Sistem ICT UTM ialah semua Ketua Bahagian di Pusat Teknologi Maklumat (PTM), UTM. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan UTM yang berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT UTM; c) Memantau aktiviti capaian harian sistem aplikasi pengguna; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menganalisis dan menyimpan rekod jejak audit; f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan	Pentadbir Sistem ICT

kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
UTM-020207 Pemilik Sistem	**Tindakan**
Pemilik Sistem merupakan PTJ yang bertanggungjawab terhadap sesuatu sistem. Peranan Pemilik Sistem adalah seperti berikut : a) Memastikan sistem beroperasi dengan baik dan lancar; b) Memastikan segala data dan maklumat di dalam sistem adalah tepat, lengkap dan boleh dipercayai; dan c) Memastikan sistem telah dilengkapi dengan langkah- langkah keselamatan melalui semakan senarai kawalan akses dan sebagainya.	Pemilik Sistem
UTM-020208 Pengguna	**Tindakan**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT UTM; 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 UTM dan menjaga kerahsiaan maklumat UTM; e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT UTM sebagaimana Lampiran 1.	Pengguna
UTM-020209 Jawatankuasa IT Universiti (JITU)	**Tindakan**
Tugas JITU: a) Menetapkan dan memperaku visi, arah tuju dan strategi ICT Universiti; b) Memperaku dan mengesahkan polisi /dasar dan prosedur berkaitan dengan pengurusan dan pentadbiran ICT Universiti;	JITU UTM

c) Mengesahkan perancangan yang disediakan oleh CICT dan lain-lain jawatankuasa; d) Mengesahkan perolehan ICT Universiti; e) Memperaku keputusan perolehan PTJ yang dibuat oleh Jwatankuasa Teknikal Perolehan ICT Universiti; f) Membincangkan isu-isu utama berkaitan ICT yang dibawa oleh ahli; g) Memperakukan pelan strategik ICT Universiti dan memantau pelaksanaannya; h) Menilai pencapaian prestasi ICT Universiti semasa; dan i) Menyelaras dan menyeragamkan pelaksanaan ICT disemua PTJ.	
UTM-020210 Pasukan Tindak Balas Insiden Keselamatan ICT UTM (UTMCERT)	**Tindakan**
Peranan dan tanggungjawab UTMCERT adalah seperti berikut: a) Menerima dan mengawasi laporan berkenaan insiden keselamatan ICT dan mencadangkan tindakan yang sesuai; b) Memberi latihan teknikal kepada pentadbir dan pengendali perkhidmatan ICT dalam aspek keselamatan ICT; c) Mengawal dan menyelaras pengurusan insiden keselamatan ICT serta menyediakan garispanduan, nasihat dan prosedur dalam aspek pengurusan keselamatan ICT pelayan/peralatan ICT dan aplikasi di UTM; d) Mengambil tindakan proaktif dan preventif dengan menyediakan infrastruktur keselamatan ICT serta melaksanakan ujian keselamatan pelayan/aplikasi kepada semua peralatan ICT/aplikasi yang disambung/guna dan akan disambung/guna di rangkaian UTM; e) Menyediakan analisis, laporan dan garispanduan teknikal yang perlu dilaksanakan jika berlaku insiden keselamatan ICT; dan f) Menyelaras respon insiden keselamatan ICT dengan pihak-pihak	UTMCERT

Commented [MM1]: Siapa ahli UTM CERT? Perlu didokumenkan didalam Manual ISMS

yang berkaitan di Malaysia seperti MyCERT, GCERT, ISPs dan agensi yang berkaitan.	

0203 Pihak Luar/Asing

Objektif:

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

UTM-020301 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	**Tindakan**
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 UTM; 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 UTM 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 dimeteraikan: • Dasar Keselamatan ICT UTM; • Tapisan Keselamatan; • Perakuan Akta Rahsia Rasmi 1972; • Hak Harta Intelek f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT UTM sebagaimana Lampiran 1.	Semua PTJ, Ketua Jabatan

0204 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif:

Memastikan setiap pengurusan projek yang dilaksanakan oleh UTM dan Jabatan di bawahnya mengambilkira aspek keselamatan maklumat secara holistik.

UTM-020401	**Tindakan**
Seksyen ini menjelaskan keperluan untuk menjadikan objektif keselamaan maklumat sebahagian daripada objektif projek; a) Melaksanakan penilaian terhadap risiko keselamatan maklumat difasa awal (pada permulaan fasa) perlaksanaan projek sebelum kawalan keselamatan yang berkaitan dikenalpasti; b) Menjadikan isu keselamatan maklumat sebagai agenda dalam setiap fasa kaedah perlaksanaan projek; c) Memastikan pengurusan projek mematuhi manual keselamatan dan polisi DKICT dalam setiap aktiviti pengurusan projek; d) Memastikan pengurus projek telah mendapat latihan kesedaran dan pendedahan yang mencukupi berkenaan tanggungjawab untuk memastikan keselamatan maklumat sentiasa terjamin; e) Memastikan aktiviti bagi menjamin keselamatan maklumat dinyatakan secara jelas dalam jadual perancangan perlaksanaan projek; f) Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian (seperti Akta Rahsia Rasmi).	Ketua PTJ

0205 Polisi Keselamatan Maklumat Berkaitan Hubungan Pembekal

Objektif:

Menjelaskan keperluan untuk mendokumentasikan strategi mitigasi risiko keselamatan maklumat bilamana pembekal dibenarkan untuk akses ke aset UTM.

UTM-020501	Tindakan
Seksyen ini menjelaskan polisi berkaitan keselamatan maklumat dan hubungan pembekal; a) Mengenalpasti dan mendokumenkan jenis-jenis pembekal (seperti khidmat servis IT, pembekal infrastruktur IT, logstik, keewangan dsb.); b) Mengenalpasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; c) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (UTM dan pembekal) untuk mendedahkan mereka dengan polisi, proses, dan prosidur berkaitan keselamatan maklumat. d) Mewujudkan mekanisma/proses pengurusan pembekal dengan mengambil kira aspek keselamatan maklumat sebagai teras; e) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan maklumat. Proses dan prosidur berkaitan perlu diwujudkan; f) Mewujudkan kontrak rasmi ersama pembekal yang dapat menjamin keselamatan maklumat UTM disamping segala urusan bersama pembekal hendaklah dilaksanakan secara rasmi; g) Memastikan pihak pembekal mewujudkan Pelan Kesinambungan Perkhidmatan dan Rancangan Pemulihan Bencana mereka khususnya jika pembekal menyediakan khidmat yang kritikal kepada UTM; h) Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semua asset maklumat	Ketua PTJ

sekiranya kontrak mereka tamat atau ditamatkan.	

0206 Rangkaian Pembekal ICT

Objektif:

Menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan maklumat berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira.

UTM-020601	**Tindakan**
Seksyen ini menjelaskan polisi berkaitan rangkaian pembekal yang meyumbang kepada sesuatu operasi atau projek yang ingin dilaksanakan; a) Mengenalpasti keperluan keselmatan maklumat khusus berkaitan dengan perolehan rangkaian pembekal servis ICT dan produk sebagai tambahan kepada keperluan umum keselamatan maklumat berkaitan hubungan pembekal yang telah dikenal pasti; b) Memastikan rangkaian pembekal yang terlibat dalam menyediakan khidmat servis ICT berkongsi hal berkaitan keselamatan maklumat (polisi, prosidur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal; c) Khusus untuk rangkaian pembekal produk, UTM perlu memastikan pembekal utama berkongsi praktis pembangunan produk UTM dikesemua peringkat pembekal bagi memastikan keselamatan maklumat terjamin; d) Melaksanakan proses pemantauan rangkaian pembekal servis ICT dan produk dengan kaedah yang berkesan bagi menjamin keperluan keselamatan maklumat sentiasa dipatuhi; e) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai; f) Mewujudkan peraturan yang khusus bagi mengawal perkongsian maklumat dikalangan rangkaian pembekal; g) Mewujudkan mekanisma/proses khusus untuk mengurus rangkaian	Ketua PTJ

pembekal khidmat servis ICT dan produk bagi memastikan keselamatan maklumat terjamin. Mekanisma yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku.	

BIDANG 03

PENGURUSAN ASET ICT

Huraian	Setiap aset ICT perlu dikenal pasti, dikelaskan, direkodkan ke dalam sistem inventori didokumenkan, diselenggarakan dan dilupuskan apabila tiba masanya.
Objektif	Untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT UTM.

0301 Pengurusan Aset ICT

Akauntabiliti Aset

Objektif:

Memastikan semua aset ICT di UTM diberi kawalan dan perlindungan yang bersesuaian.

UTM-030101 Inventori Aset ICT	**Tindakan**
Ini bertujuan memastikan semua asset 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 makluman aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; b) Memastikan semua asset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Jabatan Perdana Menteri; d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di	Pentadbir Sistem dan Semua PTJ

bawah kawalannya.	

0302 Tanggungjawab Ke Atas Aset ICT

Objektif:

Seksyen ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

UTM-030201 Tanggungjawab Ke Atas Aset ICT	**Tindakan**
Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset ICT di rekod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini dalam Sistem Pengurusan Aset; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan c) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; d) Memastikan pengurusan aset ICT yang meliputi penyelenggaraan dan pelupusan hendaklah mematuhi peraturan yang telah ditetapkan.	CICT, Pengurus Fasiliti , Pejabat Bendahari dan Ketua Jabatan

0303 Pengelasan Maklumat

Objektif:

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.

UTM-030301 Pengelasan Maklumat	**Tindakan**
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	Pejabat Pendaftar, Pejabat Bendahari dan Semua PTJ

0304 Pelabelan Dan Pengendalian Maklumat

Objektif:

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah

UTM-030401 Pengendalian Maklumat	**Tindakan**
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 standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan	Semua PTJ

Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

BIDANG 04

KESELAMATAN SUMBER MANUSIA

Huraian	Semua peranan dan tanggungjawab warga UTM, pembekal, pakar runding dan pihak-pihak lain terhadap keselamatan ICT hendaklah jelas dan didokumenkan mengikut keperluan Dasar Keselamatan ICT UTM.
Objektif	Untuk memastikan semua sumber manusia yang terlibat termasuklah warga UTM, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan ICT UTM.

0401 Keselamatan Sumber Manusia	
Objektif: Peranan dan tanggungjawab terhadap keselamatan sumber manusia	
UTM-040101 Tanggungjawab Keatas Sumber Manusia	**Tindakan**
Ketua Jabatan adalah bertanggungjawab ke atas sumber manusia yang terlibat secara langsung atau tidak langsung dalam pengendalian aset ICT di bawah kawalannya.	Ketua Jabatan dan Pejabat Pendaftar

0402 Sebelum Berkhidmat

Objektif:

Peranan dan tanggungjawab pegawai dan kakitangan sebelum, semasa dan selepas perkhidmatan

UTM-040201 Sebelum Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan UTM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan UTM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

0403 Dalam Perkhidmatan

Objektif:

Peranan dan tanggungjawab pegawai dan kakitangan sebelum, semasa dan selepas perkhidmatan

UTM-040301 Dalam Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan UTM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh UTM;	Semua

b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT UTM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau undang- undang ke atas pegawai dan kakitangan UTM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh UTM; 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. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Sumber Manusia, UTM.	

0404 Bertukar Atau Tamat Perkhidmatan	
Objektif: Peranan dan tanggungjawab pegawai dan kakitangan sebelum, semasa dan selepas perkhidmatan	
UTM-040401 Bertukar atau Tamat Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Memastikan semua aset ICT dikembalikan kepada UTM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan UTM dan/atau terma perkhidmatan.	Semua

0405 Program Kesedaran, Pendidikan Dan Latihan Keselamatan ICT	
Objektif: Setiap pengguna perlu diberikan kesedaran, latihan atau kursus mengenai keselamatan ICT yang bersesuaian dengan peranan dan tanggungjawab masing-masing secara berterusan.	
UTM-040501 Program Kesedaran, Pendidikan Dan Latihan Keselamatan ICT	**Tindakan**
Program menangani insiden juga penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT UTM.	CICT dan Pengurus Fasiliti

BIDANG 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Huraian	Premis dan peralatan memproses maklumat yang kritikal dan sensitif hendaklah ditempatkan di kawasan yang selamat dan dilindungi dari sebarang ancaman fizikal dan persekitaran.
Objektif	Untuk menghalang capaian yang tidak dibenarkan, kerosakan dan gangguan terhadap persekitaran premis, peralatan dan maklumat.

0501 Keselamatan Fizikal Dan Persekitaran	
UTM-050101 Kawalan Kawasan	**Tindakan**
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat universiti. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja	Pengarah Keselamatan UTM, PHB, CIO, ICTSO dan OSHE

boleh melalui pintu masuk ini; i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	

0502 Kawalan Kawasan Terhad	
UTM-050201 Kawalan Masuk Fizikal	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Setiap warga UTM hendaklah memakai atau mengenakan kad metrik staf atau kad metrik pelajar sepanjang waktu bertugas; b) Semua kad metrik staf dan kad metrik hendaklah diserahkan balik kepada universiti apabila berhenti atau bersara; c) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di pintu masuk UTM atau tempat berurusan dan pas ini hendaklah dikembalikan semula selepas tamat lawatan; d) Kehilangan pas estilah dilaporkan dengan segera kepada pihak Keselamatan UTM dan OSHE;	Semua
UTM-050202 Kawasan Larangan	**Tindakan**
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di UTM adalah bilik Naib Canselor, bilik-bilik Timbalan Naib	Pentadbir Sistem

Canselor, Pusat Data dan Bilik Rangkaian. Akses kepada kawasan larangan hanyalah kepada pegawai- pegawai yang dibenarkan sahaja; dan Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	

0503 Kawalan Peralatan

UTM-050301 Peralatan ICT Pengguna	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian,	Semua

kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

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

j) Semua peralatan ICT 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 rak khas dan berkunci;

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

l) Peralatan ICT yang hendak dibawa keluar dari premis UTM, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT;

t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

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

Commented [MM2]: Boleh jadi perangkap semasa audit. Bagus kalau dirutinkan tetapi kalau auditor dapat detect ada perkakasa tidak ditutup, mereka boleh bagi RFI kalau tak NC (Dikuatkuasakan dalam Polisi)

v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan w) Memastikan plag dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	

Commented [MM3]: ditto

0504 Infrastruktur Sokongan	
UTM-050401 Infrastruktur Sokongan	**Tindakan**
a) Kawalan Persekitaran Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT UTM, semua cadangan perolehan dan pengubahsuaian fizikal hendaklah dirujuk terlebih dahulu kepada Pejabat Harta Bina (PHB). Perkara yang perlu dipatuhi adalah seperti berikut : ▪ Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat; ▪ Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; ▪ Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan; ▪ Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT; ▪ Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT; ▪ Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran perkakasan komputer; dan ▪ Menyemak dan menguji semua infrastruktur sokongan sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	CICT, PHB, OSHE, TNCP, Pejabat Pendaftar dan semua PTJ

b) Bekalan Kuasa

Melindungi semua peralatan ICT UTM dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;

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

Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

c) Utiliti

Semua kemudahan utiliti seperti penghawa dingin, bekalan air, kumbahan dan pengalihan udara perlu dilindungi dari kegagalan bekalan elektrik dan sebarang gangguan; dan

Kemudahan utiliti perlu diperiksa dan diuji agar sentiasa berfungsi dengan baik bagi mengurangkan risiko kegagalan;

d) Prosedur Kecemasan

Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh TNCP dan Pengarah Keselamatan UTM;

Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan UTM

Mewujudkan, menguji dan mengemas kini pelan kecemasan dari masa ke semasa; dan

Mengadakan latihan fire drill mengikut jadual secara berkala.

Keselamatan Kabel Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi daripada pencerobohan dan kerosakan. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

- Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
- Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan

▪ Membuat pelabelan kabel menggunakan kod tertentu.	

0505 Penyelenggaran Peralatan	
UTM-050501 Penyelenggaraan Perkakasan	**Tindakan**
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh 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; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan aset ICT mestilah mendapat kebenaran daripada Pengurus ICT.	CICT dan Semua PTJ

0506 Peminjaman Perkakasan Untuk Kegunaan Luar Pejabat	
UTM-050601 Peminjaman perkakasan	**Tindakan**
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko.	Unit Keselamatan

Langkah-langkah keselamatan yang perlu diambil tetapi tidak hanya terhad kepada perkara berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Universiti bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan; b) Melindungi dan mengawal peralatan sepanjang masa; c) Merekodkan aktiviti peminjaman dan pemulangan peralatan mengikut peraturan yang telah ditetapkan; dan d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik.	dan Ketua PTJ

0507 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar	
UTM-050701 Peralatan di Luar Premis	**Tindakan**
Perkakasan yang dibawa keluar dari premis UTM adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua

0508 Pelupusan Peralatan	
UTM-050801 Pelupusan Perkakasan ICT	**Tindakan**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh UTM dan ditempatkan di UTM. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa.	PHB, Bendahari, Unit Keselamatan, Unit Undang-

Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan UTM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Data-data dalam storan peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan telah dihapuskan dengan cara yang selamat; d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Harta Bersepadu; g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; c) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di UTM; d) Memindah keluar dari UTM mana-mana peralatan ICT yang hendak dilupuskan; e) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di	undang dan CICT

bawah tanggungjawab UTM; dan f) 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.	

0509 Clear Desk dan Clear Screen	
UTM-050901 Prosedur Clear Desk dan Clear Screen	**Tindakan**
Prosedur Clear Desk dan Clear Screen perlu dipatuhi supaya maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan salah guna, kerosakan, kecurian atau kehilangan. Langkah-langkah keselamatan yang perlu diambil tetapi tidak hanya terhad kepada perkara berikut: a) Menggunakan kemudahan password screen saver atau logout domain controller apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci, kabinet fail dan bilik yang berkunci; c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; dan d) Memastikan semua dokumen yang terdapat dalam memori pencetak, pengimbas, mesin faksimile, mesin fotostat dan mobile devices dipadam.	Semua PTJ, Ketua Jabatan, Pejabat Pendaftar dan CICT

BIDANG 6

PENGURUSAN OPERASI DAN KOMUNIKASI

Huraian	Prosedur pengurusan operasi dan komunikasi hendaklah didokumenkan, diselenggarakan dan mudah didapati apabila diperlukan.
Objektif	Untuk memastikan kemudahan pemprosesan maklumat dan komunikasi sentiasa berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

0601 Pengurusan Operasi Dan Komunikasi

Pengurusan Prosedur Operasi

Objektif :

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

UTM-060101 Pengendalian Prosedur	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih 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 dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua

0602 Tanggungjawab Dan Prosedur Operasi	
UTM-060201 Kemudahan Tanggungjawab Dan Prosedur Operasi	**Tindakan**
Seksyen ini bertujuan memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan. Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas lagi teratur, dikemas kini dan sedia diguna pakai oleh pengguna mengikut keperluan; b) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal; c) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset; dan d) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	Ketua Jabatan, CICT dan Unit undang-undang

0603 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding Dan Yang Berkaitan	
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.	
UTM-060301 Perkhidmatan Penyampaian	**Tindakan**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan	ICTSO, Pentadbir Sistem

dan disenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

0604 Perancangan Dan Penerimaan Sistem	
Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
UTM-060401 Perancangan Kapasiti	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT 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.	ICTSO, Pentadbir Sistem
UTM-060402 Penerimaan Sistem	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. b) Ujian yang sesuai ke atas sistem baru perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.	ICTSO, Pentadbir Sistem

0605 Perlindungan Dari Kod Perosak Dan Mobile Code

Perisian Berbahaya

Objektif:

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

UTM-060501 Perlindungan dari Perisian Berbahaya	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, 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 antivirus sebelum menggunakannya; d) Mengemas kini 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 mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan	Semua

virus.	
UTM-060502 Perlindungan dari Mobile Code	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

0606 Penduaan (Backup)

Housekeeping

Objektif:

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

UTM-060601 Pematuhan Penduaan (Backup)	**Tindakan**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan (backup) hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di off site. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; 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 secara berkala bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	CICT

0607 Pengurusan Keselamatan Rangkaian

Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

UTM-060701 Kawalan Infrastruktur Rangkaian	**Tindakan**
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 Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi; e) Firewall hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi universiti serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan UTM; g) Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UTM;	Pentadbir Sistem

i) Memasang Web Content Filtering pada Internet Gateway untuk menyekat aktiviti yang dilarang; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan UTM adalah tidak dibenarkan; k) Semua pengguna hanya dibenarkan menggunakan rangkaian UTM sahaja. Penggunaan modem adalah dilarang sama sekali; dan l) Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan.	

0608 Pemantauan Rangkaian Berpusat	
UTM-060801 Pematuhan Pemantauan Rangkaian Berpusat	**Tindakan**
Seksyen ini bertujuan untuk memastikan pemantauan rangkaian berpusat UTM dapat berfungsi secara berkesan dan berterusan. Perkara-perkara yang mesti dipatuhi tetapi tidak hanya terhad kepada yang berikut: a) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; b) Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi; dan c) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan UTM/jabatan.	Bahagian Infrastuktur dan Operasi CICT

0609 Pengendalian Media	
Pengurusan Media	
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
UTM-060901 UTM- Penghantaran dan Pemindahan	**Tindakan**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
UTM-060902 Prosedur Pengendalian Media	**Tindakan**
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.	Semua
UTM-060903 Keselamatan Sistem Dokumentasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan seperti berikut : i. Kerahsiaan – maklumat tidak boleh didedahkan sewenang-	ICTSO, Pentadbir Sistem

wenangnya atau dibiarkan diakses tanpa kebenaran ii. Integriti – data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan. iii. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal. iv. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya v. Kebolehsediaan – data dan maklumat hendaklah boleh diakses pada bila –bila masa. b) Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	
UTM-060904 Media Storan	**Tindakan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Akses dan pergerakan media storan hendaklah direkodkan; f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan atau penduaan (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan	Semua

dengan teratur dan selamat; dan i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
UTM-060905 Media Tandatangan Digital	**Tindakan**
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.	Semua
UTM-060906 Media Perisian dan Aplikasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan UTM; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; 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.	Semua

0610 Pertukaran Maklumat

Pengurusan Pertukaran Maklumat

Objektif :

Memastikan keselamatan pertukaran maklumat dan perisian antara Jabatan Perdana Menteri dan agensi luar terjamin.

UTM-061001 Pertukaran Maklumat	Tindakan
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 UTM dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari UTM; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua

0611 Perkhidmatan Perdagangan Elektronik

Perkhidmatan E-Dagang (Electronic Commerce Services)

Objektif :

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

UTM-061101 E-Dagang	Tindakan
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik,	Semua

pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (on-line) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	

0612 Pemantauan Aktiviti Pemprosesan Maklumat	
Pemantauan	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
UTM-061201 Pengauditan dan Forensik ICT	**Tindakan**
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT UTM; 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,	ICTSO

berunsur fitnah dan propaganda; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan h) Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
UTM-061202 Jejak Audit	**Tindakan**
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 (sekurang-kurangnya enam (6) bulan). Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem
UTM-061203 Sistem Log	**Tindakan**
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:	Pentadbir

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 hendaklah melaporkan kepada CIO dan ICTSO.	Sistem
UTM-061204 Pemantauan Log	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa sekurang-kurangnya enam (6) bulan 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 UTM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Sistem, CCMC

0613 Keselamatan Komunikasi: Internet	
UTM-061301 Hak Akses Internet	**Tindakan**
Hak akses menggunakan perkhidmatan internet UTM hendaklah dilihat sebagai satu kemudahan yang disediakan oleh UTM untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang disediakan. Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk	CICT, Ketua Jabatan

maklumat) adalah Hak Milik Kerajaan~~;~~

Laman web yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan. Kategori laman yang ditegah capaian adalah seperti berikut:

- Pornography & Nudity;
- Adult & Mature Content;
- Gay & Lesbian;
- Games;
- Gambling;
- Chat, Instant Messaging & Social Networking;
- Spam URLs; dan
- Spyware.

Kecuali atas sebab-sebab kerja, kajian dan penyelidikan yang dibenarkan oleh Naib Canselor / Ketua Jabatan. Pihak CICT akan membuka laman web / portal yang diluluskan mengikut kaedah whitelist.

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

Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan atau pegawai yang diberi kuasa sebelum dimuat naik ke Internet;

Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar, sumber terbuka (OSS) dan di bawah Hak Cipta Terpelihara. Pengguna adalah dilarang memuat naik, memuat turun, menyimpan dan menggunakan perisian yang tidak sah (pirated software);

Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UTM;

a) Pengguna adalah dilarang menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah;

b) Pengguna adalah dilarang menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan

fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan serta orang awam;

c) Pengguna adalah dilarang memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;

d) Pengguna adalah dilarang memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian (streaming) seperti permainan elektronik, video dan lagu. Ia boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer (melibatkan penggunaan bandwitdh yang tinggi);

e) Pengguna adalah dilarang menyebarkan maklumat rasmi dengan menggunakan kemudahan chatting atau instant messaging

f) Pengguna adalah dilarang menggunakan kemudahan Internet untuk tujuan peribadi seperti laman web blog individu;

g) Pengguna adalah dilarang menjalankan aktiviti-aktiviti komersial seperti jualan langsung, skim pelaburan internet, politik dan sebagainya;

h) Pengguna adalah dilarang melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata, aktiviti pengganas dan sebagainya yang boleh mengancam kepada kesejahteraan dan ketenteraman awam;

i) Pengguna yang diberi kebenaran untuk memuat naik, memuat turun, menghantar (file-transfer-protocol) dan menyimpan kad elektronik, video, lagu dan kepilan fail hendaklah tidak melebihi saiz lima (5) megabait.

j) Pengguna adalah dilarang menggunakan kemudahan modem peribadi, streamyx dan access point (wireless) untuk membuat capaian terus ke Internet kecuali setelah mendapat kebenaran daripada Naib Canselor / Ketua Jabatan atau pegawai yang diberi kuasa;

k) Pengguna tidak boleh membiarkan komputer berada atas talian (on-line) jika tidak digunakan. Log off komputer sebelum keluar pejabat supaya tidak disalah gunakan oleh mana-mana pihak;

l) Mana-mana pengguna termasuk pihak luar adalah dilarang menggunakan sebarang peralatan komputer membabitkan storan luar untuk tujuan muat turun/naik maklumat internet seperti thumb/pen drive, disket,

CDRW, DVD writetable dan external hard disk sebelum diimbas terlebih dahulu dengan sebarang produk anti-malware (virus, worms, trojan backdoor, spyware dsb.) bagi mengelakkan malware outbreak di rangkaian UTM dan berlaku insiden keselamatan ICT; dan m) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	

0614 Keselamatan Komunikasi: Mel Elektronik/E-Mail

UTM-061401 Pengurusan Mel Elektronik (E-mel)	**Tindakan**
Penggunaan e-mel di UTM hendaklah dipantau secara berterusan oleh Pentadbir E-mel 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 UTM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh UTM; c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e- mel rasmi dan pastikan alamat e-mel penerima adalah betul; e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak	Semua

melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

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

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

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

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

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

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

l) Pengguna hendaklah memastikan alamat e-mel persendirian yang tidak dibenarkan oleh pihak UTM tidak boleh digunakan untuk tujuan rasmi; dan

m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.

0615 Bawa Peranti Dan Teknologi Sendiri (BYOD)

UTM-061501 Kebenaran Bawa Peranti dan Teknologi Sendiri (BYOD)	Tindakan
Peranti peribadi yang dibenarkan untuk digunakan seperti komputer riba, telefon pintar, dan tablet untuk tujuan rasmi perlu didaftarkan dan perlu mematuhi peraturan semasa; Pengguna tertakluk kepada syarat dan polisi yang ditetapkan di dalam Dasar Keselamatan ICT UTM; dan Warga UTM boleh melayari internet dari wifi hotspot UTM dengan menggunakan ACID akaun. Capaian tanpa menggunakan akaun pengguna yang sah adalah melanggar polisi Dasar Keselamatan ICT UTM.	CICT , Semua PTJ

BIDANG 07

KAWALAN CAPAIAN

Huraian	Capaian ke atas maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem.
Objektif	Untuk mengawal capaian ke atas maklumat.

0701 Pengurusan Kawalan Capaian

UTM-070101 Kawalan Capaian	**Tindakan**
Ketua Jabatan adalah bertanggungjawab untuk memastikan kawalan capaian ke atas aset ICT termasuk maklumat, perkhidmatan rangkaian dan kemudahan-kemudahan yang berkaitan diwujudkan dan dilaksanakan dengan berkesan berasaskan keperluan urusan dan keselamatan.	Ketua Jabatan

0702 Keperluan Kawalan Capaian

UTM-070201 Pematuhan Kawalan Capaian	**Tindakan**
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	ICTSO, CICT

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.	

0703 Pengurusan Akaun Pengguna	
Pengurusan Capaian Pengguna	
Objektif : Mengawal capaian pengguna ke atas aset ICT Universiti Teknologi Malaysia.	
UTM-070301 Akaun Pengguna	**Tindakan**
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara- perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh UTM sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna yang diwujudkan 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 UTM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna	Semua, Pentadbir Sistem

atas sebab-sebab berikut: ▪ Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ▪ Bertukar bidang tugas kerja; ▪ Bertukar ke agensi lain; ▪ Bersara; atau ▪ Ditamatkan perkhidmatan.	

0704 Tanggungjawab Pengguna

UTM-070401 Tanggungjawab Pengguna	**Tindakan**
Semua pengguna yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada ICTSO, kerentanan (vulnerability) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.	ICTSO, Semua

0705 Kawalan Capaian Rangkaian

UTM-070501 Capaian Rangkaian	**Tindakan**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian UTM, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap	ICTSO, Pentadbir Sistem

perkhidmatan rangkaian ICT.	

0706 Kawalan Capaian Sistem Pengoperasian	
Kawalan Capaian Sistem Pengoperasian	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
UTM-070601 Capaian Sistem Pengoperasian	**Tindakan**
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian 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; dan b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan c) Menjana amaran (alert) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Mengehadkan dan mengawal penggunaan program; dan	ICTSO, Pentadbir Sistem

d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

0707 Kawalan Capaian Sistem Aplikasi

Kawalan Capaian Aplikasi dan Maklumat

Objektif :

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

UTM-070701 Capaian Aplikasi dan Maklumat	**Tindakan**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	ICTSO, Pentadbir Sistem

0708 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif :

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

UTM-070801 Peralatan Mudah Alih	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan b) Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
UTM-070802 Kerja Jarak Jauh	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti berikut: Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

0709 Kawalan Capaian Sistem Pangkalan Data

UTM-070901 Capaian Sistem Pangkalan Data	**Tindakan**
Seksyen ini bertujuan untuk memastikan capaian ke atas pangkalan data dan data dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong pengesahan pengguna, mewujudkan jejak audit ke atas semua capaian, menjana amaran (alert), pengesahan capaian dan penyimpanan data. Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada perkara berikut: a) Capaian ke atas pangkalan data hendaklah dikawal.	

b) Penggunaan perisian yang membolehkan capaian terus ke pangkalan data secara pihak ketiga sama ada melalui perisian web (cth : phpmyadmin) atau sebagainya adalah tidak dibenarkan. c) Mewujudkan pengenalan diri (ID) yang unik bagi setiap pengguna dan hanya digunakan untuk pengguna berkenaan sahaja. d) Aplikasi yang perlu mengakses ke pangkalan data perlu menggunakan pengenalan diri yang berbeza daripada pengenalan diri pembangun aplikasi dan pentadbir pangkalan data.	

BIDANG 08

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SIS. MAKLUMAT

Huraian	Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat sedia ada atau sistem maklumat baru hendaklah menyatakan keperluan-keperluan kawalan keselamatan.
Objektif	Untuk memastikan aspek keselamatan dikenal pasti dan diambil kira dalam semua sistem maklumat dan/atau perkhidmatan termasuk sistem pengoperasian, infrastruktur, sistem aplikasi dan sistem perisian. Aspek keselamatan ini mesti dikenal pasti, dijustifikasikan, dipersetujui dan didokumentasikan sebelum sesuatu sistem maklumat direka bentuk dan dilaksanakan.

0801 Perolehan Pembangunan Dan Penyelenggaraan Sistem Maklumat	
UTM-080101 Perolehan Sistem Maklumat	**Tindakan**
Ketua PTJ adalah bertanggungjawab untuk: a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat; b) Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu; c) Memastikan sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat; dan d) Menjaga dan menjamin keselamatan sistem maklumat.	Ketua PTJ

0802 Keperluan Keselamatan Sistem Maklumat	
UTM-080201 Pematuhan Keselamatan Sistem Maklumat	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira 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 sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	ICTSO, Pemilik Sistem, Pentadbir Sistem

0803 Pemprosesan Aplikasi Dengan Tepat	
UTM-080301 Pematuhan Pemprosesan Aplikasi Dengan Tepat	**Tindakan**
Seksyen ini bertujuan memastikan kawalan keselamatan yang sesuai diolah dan diterapkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi. Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut: a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam	

aplikasi bagi menjamin kesahihan dan ketepatan; b) Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenal pasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan; c) Mengenal pasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan d) Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi.	

0804 Kawalan Kriptografi	
Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
UTM-080401 Enkripsi	**Tindakan**
Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
UTM-080402 Tandatangan Digital	**Tindakan**
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
UTM-080403 Pengurusan Infrastruktur Kunci Awam (PKI)	**Tindakan**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

0805 Keselamatan Fail-Fail Sistem	
Keselamatan Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
UTM-080501 Kawalan Fail Sistem	**Tindakan**
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 atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian 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 pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, Pentadbir Sistem

0806 Keselamatan Dalam Proses Pembangunan Dan Sokongan	
Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
UTM-080601 Prosedur Kawalan Perubahan	**Tindakan**
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 diguna pakai;	Pemilik Sistem, Pentadbir Sistem

b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan universiti. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; 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.	
UTM-080602 Pembangunan Perisian Secara Outsource	**Tindakan**
Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik UTM.	Bahagaian Pembangunan Aplikasi dan Semua PTJ

0807 Pengurusan Penilaian Kerentanan (SPA)	
UTM-080701 Perlaksanaan Pengurusan Penilaian Kerentanan	**Tindakan**
Seksyen ini bertujuan memastikan pelaksanaan pengurusan penilaian kerentanan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya. Pelaksanaan pengurusan penilaian keterdedahan ini perlu juga dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan sekurang-kurangnya setahun sekali bergantung kepada tahap kritikal sistem pengoperasian dan sistem aplikasi yang sedia ada.	ICTSO

0808 Sekatan Dalam Instalasi Perisian	
UTM-080801 Peraturan Instalasi Perisian	**Tindakan**
Seksyen ini menjelaskan peraturan berhubung instalasi perisian yang perlu diwujud dan dilaksanakan. Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut: Pengguna hanya dibenarkan menggunakan perisian yang disediakan oleh CICT sahaja kecuali perisian yang mendapat persetujuan Ketua PTJ masing-masing atas tujuan rasmi.	CICT dan Semua

0809 Polisi Pembangunan Sistem Selamat	
UTM-080901 Keselamatan Pembangunan Sistem Selamat	**Tindakan**
Seksyen ini berperanan untuk memastikan keselamatan maklumat direkabentuk dan dilaksanakan didalam kerangka pembangunan sistem maklumat. Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut: a) Mewujudkan persekitaran yang selamat untuk pembangunan sistem maklumat; b) Mewujudkan garis panduan jelas perihal keselamatan maklumat didalam proses pembangunan perisian/sistem maklumat; c) Mengenalpasti keperluan keselamatan didalam fasa rekabentuk perisian/sistem maklumat; d) Mengadakan titik semakan keselamatan didalam jadual perbatuan projek pembangunan perisian/sistem maklumat; e) Mewujudkan repositori yang selamat untuk perisian/sistem maklumat yang dibangunkan;	Semua

f) Memastikan keselamatan dalam kawalan versi; g) Mengenalpasti aplikasi yang diperlukan untuk merekod pengetahuan berkaitan keselamatan sistem maklumat; h) Membina kemahiran pembangun perisian/sistem maklumat supaya mereka mampu menjauhi, mengenalpasti, dan merungkai setiap kelemahan yang dikesan didalam perisian/sistem maklumat yang dibangunkan. Teknik pengaturcaraan selamat wajar dipraktik; i) Piawaian tentang teknik pengaturcaraan selamat wajar dirujuk; j) Kumpulan pembangun perlu diberi latihan secukupnya tentang skil pengujianan dan penyemakan kod perisian; k) Jika pembangunan perisian dilaksanakan dengan menggunakan sumber luar, CICT perlu mendapatkan jaminan bahawa pemaju yang dilantik memenuhi peraturan, polisi, prosidur, dan proses berkaitan pembangunan sistem selamat.	

0810 Prinsip Kejuruteraan Sistem Selamat	
UTM-081001 Kepentingan Prinsip Kejuruteraan Sistem Selamat	**Tindakan**
Seksyen ini menjelaskan kepentingan untuk mewujud, mendokumen, dan menyelenggara prinsip-prinsip kejuruteraan sistem maklumat untuk digunapakai sewaktu pembangunan sistem maklumat. Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut: a) Prosedur kejuruteraan sistem maklumat selamat yang berasaskan kepada prinsip- prinsip keselamatan kejuruteraan sistem perlu dibangun, didokumen, dan dilaksana di dalam setiap projek pembangunan sistem maklumat; b) Aspek keselamatan perlu perlu diberi penekanan dalam setiap lapisan rekabentuk struktur sistem maklumat (seperti lapisan bisnes, lapisan data, dan lapisan applikasi);	Semua

c) Setiap teknologi baru yang bakal diguna pakai oleh UTM perlu dianalisis bagi menilai risiko keselamatan. Rekabentuk teknologi perlu disemak dari sudut kelemahan dan potensi serangan oleh penceroboh sistem maklumat; d) Setiap prosedur dan prinsip kejuruteraan sistem maklumat yang dibangunkan perlu disemak dari masa ke semasa bagi memastikan ianya kekal relevan dan mampu menangani ancaman keselamatan yang sentiasa berubah mengikut masa; e) Prinsip dan prosedur kejuruteraan sistem selamat juga perlu digunapakai sekiranya UTM melaksanakan pembangunan sistem maklumat mengunakan sumber luar. Pematuhan kepada prinsip dan prosidur berkaitan perlu dinyatakan dengan jelas dalam perjanjian bersama pemaju luar.	

0811 Persekitaran Pembangunan Sistem Selamat	
UTM-081101 Keperluan Persekitaran Pembangunan Sistem Maklumat	**Tindakan**
Seksyen ini menjelaskan keperluan untuk memastikan persekitaran pembangunan sistem adalah selamat dan dilindungi bagi memastikan pembangunan, pengintegrasian, dan pengujianan sistem maklumat terjamin. Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut: a) Sensitiviti data yang perlu diproses, disimpan, dan dipindahkan melalui sistem maklumat yang dibangunkan; b) Keperluan dalaman dan luaran yang berkaitan (seperti regulasi dan polisi); c) Kawalan keselamatan yang telah sedia laksana dalam CICT yang menyokong aktiviti pembangunan sistem maklumat; d) Kebolehpercayaan personel yang bekerja dalam persekitaran pembangunan sistem maklumat; e) Tahap penglibatan suber luar dalam pembangunan sistem maklumat;	Semua

f) Keperluan untuk mengasingkan beberapa persekitaran yang berbeza; g) Kawalan akses ke persekitaran pembangunan sistem malumat; h) Pemantauan perubahan terhadap persekitaran dan kod sumber; i) Pendua kepada data-data projek pembangunan sistem maklumat disimpan di lokasi berasingan dari persekitaran pembangunan sistem maklumat; j) Kawalan terhadap pergerakan data dari dan kepada persekitaran; k) Setelah strategi perlindungan persekitaran ditentukan, UTM sewajarnya mendokumenkan proses-proses yang berkaitan didalam kerangka pembangunan sistem selamat dan menjadikannya sebagai rujukan kumpulan pemaju.	

0812 Pengujianan Keselamatan Sistem	
UTM-081201 Pengujian Keselamatan ICT	**Tindakan**
Seksyen ini menjelaskan keperluan untuk melaksanakan pengujian terhadap fungsi-fungsi keselamatan sistem maklumat semasa fasa pembangunan berlangsung. Perkara-perkara yang perlu diambilkira tetapi tidak hanya terhad kepada yang berikut: a) Persiapan rapi untuk melaksanakan pengujianan keselamatan sistem maklumat perlu dilakukan termasuk jadual pengujianan, data input, jangkaan keputusan, dan kondisi pengujianan; b) Untuk sistem maklumat yang dibangunkan sepenuhnya oleh KDN, pengujianan keselamatan sistem maklumat boleh dilakukan oleh kumpulan dalaman terlebih dahulu kemudian baru diikuti dengan pengujianan penerimaan secara bebas oleh pengguna sebenar sistem.	Semua

BIDANG 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Huraian	Semua insiden keselamatan ICT yang berlaku di UTM mestilah dilaporkan dengan serta-merta kepada UTM CERT dan dikendalikan mengikut peraturan atau prosedur pengurusan pengendalian insiden keselamatan ICT Kerajaan yang ditetapkan.
Objektif	Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan, dan memastikan sistem ICT UTM dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej UTM.

0901 Pengurusan Pengendalian Insiden Keselamatan ICT	
UTM-090101 Pengurusan Insiden Keselamatan ICT	**Tindakan**
Ketua PTJ adalah bertanggungjawab untuk memastikan Bahagian / Seksyen / Unit di bawah kawalannya mematuhi dasar mengenai pengurusan pengendalian insiden keselamatan ICT UTM dengan merujuk kepada UTM CERT, pekeliling am, surat pekeliling am, garis panduan dan prosedur operasi standard yang telah dikeluarkan oleh Kementerian dan Kerajaan.	Ketua PTJ

0902 Insiden Keselamatan ICT	
UTM-090201 Laporan Insiden Keselamatan ICT	**Tindakan**
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	Semua

UTM CERT 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.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di UTM sepertimana Lampiran 2.

Commented [MM4]: Perlu disertakan (Dapatan dari GCERT Pengurusan Insiden) Dr Murtada – Lampiran 2

0903 Mekanisma Pelaporan Insiden Keselamatan ICT

Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

UTM-090301 Mekanisme Pelaporan	**Tindakan**
Mekanisma pelaporan berikut wajar dilaksanakan bila mana insiden keselamatan ICT berlaku: a) Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pegawai Keselamatan ICT (ICTSO) UTM dan kepada UTM CERT atau / dan kepada Government Computer Emergency Response Team (GCERT) untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan.	Semua

Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. b) Pelantikan Pegawai Bertanggungjawab Pegawai Keselamatan ICT UTM atau ICTSO dan anggota pasukan UTM CERT mestilah dilantik secara rasmi oleh pengurusan UTM, dan semua warga UTM perlu ambil maklum akan pelantikan pegawai-pegawai ini, dan perlu sentiasa bersedia untuk memberi respons apabila diperlukan. c) Tanggungjawab Pengguna Semua warga UTM, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat UTM menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan pencerobohan. d) Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak kepada agensi-agensi lain. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di UTM sepertimana Lampiran 2.	

0904 Prosedur Pengendalian Insiden Keselamatan ICT	
UTM-090401 Prosedur Pelaporan Insiden Keselamatan ICT	**Tindakan**
Prosedur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan	Semua

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

0905 Pengurusan Maklumat Insiden Keselamatan ICT	
Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif : Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
UTM-090501 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	**Tindakan**
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 UTM. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira 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; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

0906 Penilaian Dan Keputusan Terhadap Insiden Keselamatan ICT	
UTM-090601 Hasil Penilaian dan Keputusan Insiden Keselamatan ICT	**Tindakan**
UTM CERT bertanggungjawab terhadap insiden keselamatan ICT dan keputusan perlu dibuat jika insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat mengikut prosidur yang ditetapkan. Pasukan yang terlibat wajar melaksanakan perkara- perkara berikut: a) Penilaian perlu dibuat berasaskan skim klasifikasi insiden yang dipersetujui; b) Insiden perlu disusun mengikut kepentingan dan implikasi kepada UTM; c) Hasil daripada penilaian yang dibuat boleh dipanjangkan kepada UTM CERT supaya pengesahan atau penilaian semula dapat dilakukan; d) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan.	ICTSO

0907 Tindakbalas Terhadap Insiden Keselamatan ICT	
UTM-090701 Matlamat Tindakbalas Insiden Keselamatan ICT	**Tindakan**
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosidur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan. Pasukan tindakbalas wajar melaksanakan perkara berikut: a) Mengumpul bahan bukti secepat yang mungkin selepas kejadian; b) Melaksanakan forensik keselamatan maklumat; c) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu; d) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk	ICTSO

analisis selanjutnya; e) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku; f) Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dengan rekod; g) Analisa pasca insiden wajar dlakukan untuk mengenalpasti punca insiden;	

BIDANG 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Huraian	Pengurusan kesinambungan perkhidmatan dan pelan pengurusan kesinambungan perkhidmatan hendaklah diwujudkan dan dilaksanakan berdasarkan kepada persekitaran dan operasi UTM.
Objektif	Untuk memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.

1001 Pengurusan Kesinambungan Perkhidmatan

UTM-100101 Kesinambungan Perkhidmatan	**Tindakan**
Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan stakeholder sistem penyampaian perkhidmatan dilindungi dan imej UTM terpelihara dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan UTM di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua PTJ adalah bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT UTM.	ICTSO Ketua PTJ

1002 Pelan Kesinambungan Perkhidmatan

UTM-100201 Pembangunan Pelan Kesinambungan Perkhidmatan	**Tindakan**
Pelan Kesinambungan Perkhidmatan (Business Continuity Management - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil	CIO, ICTSO,

bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Majlis ICT UTM. Perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes 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 backup; dan g) Menguji dan mengemas kini 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 personel UTM dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel 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.	Pengurus IT

f) 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 bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

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

h) UTM hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

BIDANG 11

PEMATUHAN

Huraian	Keperluan-keperluan perundangan, peraturan atau ikatan kontrak hendaklah dinyatakan, didokumenkan dan dikemas kini.
Objektif	Untuk menghindar pelanggaran undang-undang jenayah dan sivil, *statutory*, peraturan atau ikatan kontrak dan sebarang keperluan keselamatan lain.

1101 Pematuhan Keperluan Perundangan

UTM-110101 Pematuhan Perundangan ICT	**Tindakan**
Bertanggungjawab untuk memastikan semua pengguna aset ICT termasuk pembekal dan pakar runding mematuhi dan seterusnya memastikan pelanggaran kepada perundangan yang berkaitan dan keperluan dasar ini dielakkan.	Ketua PTJ, Unit Undang-Undang

1102 Pematuhan Dasar

UTM-110201 Pematuhan Dasar Keselamatan ICT	**Tindakan**
Setiap pengguna di UTM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT UM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di UTM termasuk maklumat yang disimpan di dalamnya adalah hak milik universiti. Ketua Jabatan/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT UTM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber UTM.	Semua

UTM-110202 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tindakan**
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 standard pelaksanaan keselamatan ICT.	ICTSO
UTM-110203 Pematuhan Keperluan Audit	**Tindakan**
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.	Semua

1103 Keperluan Perundangan

UTM-110301 Pematuhan Perundangan Keselamatan ICT	**Tindakan**
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di UTM: a) Arahan Keselamatan; b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002; d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian	Semua

Risiko Keselamatan Maklumat Sektor Awam;

g) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

j) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi- Agensi Kerajaan yang bertarikh 23 November 2007;

k) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

n) Akta Tandatangan Digital 1997;

o) Akta Rahsia Rasmi 1972;

p) Akta Jenayah Komputer 1997;

q) Akta Hak Cipta (Pindaan) Tahun 1997;

r) Akta Komunikasi dan Multimedia 1998;

s) Perintah-Perintah Am;

t) Arahan Perbendaharaan;

u) Arahan Teknologi Maklumat 2007;

v) Garis Panduan Keselamatan MAMPU 2004;

w) Standard Operating Procedure (SOP) ICT MAMPU;

x) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; dan y) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	

1104 Pelanggaran Perundangan	
UTM-110401 Pelanggaran Dasar	**Tindakan**
Pelanggaran Dasar Keselamatan ICT UTM boleh dikenakan tindakan tatatertib.	Semua

1105 Kebolehsediaan Fasiliti Pemprosesan Maklumat	
UTM-110501 Kebolehsediaan Fasiliti Pemprosesan Maklumat	**Tindakan**
Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat ditahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) perlu diwujudkan. Untuk tujuan itu, perkara berikut wajar diberi tumpuan: a) UTM perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat); b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan; c) Fasiliti pemprosesan bertindan perlu diuji bagi memastikan kesiapsediaan menjalankan operasi apabila pemprosesan utama gagal berfungsi; d) Kewujudan pemprosesan bertindan boleh membawa risiko kepada kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu	Semua

diambil kira semasa sesuatu sistem maklumat itu direkabentuk	

GLOSARI	
Risiko	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
Penilaian Risiko	Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Ancaman	Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Vulnerability	Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
Insiden Keselamatan	Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem maklumat.
Aset ICT	Bermaksud semua yang mempunyai nilai kepada organisasi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Clear Desk	Bermaksud tidak meninggalkan sebarang dokumen yang sensitif di atas meja.
Clear Screen	Bermaksud tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.
Mobile Code	Bermaksud kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetic, ooptical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.

GLOSARI	
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Denial of Service	Halangan pemberian perkhidmatan.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian ataukombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya.Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.

GLOSARI	
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
UTMCERT	*University of Technology Malaysia Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT UTM. Pasukan yang ditubuhkan untuk membantu UM mengurus pengendalian insiden keselamatan ICT di semua PTj.

RUJUKAN	VERSI	TARIKH	MUKA SURAT
DKICT	1.0	xxx	99

GLOSARI	
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.