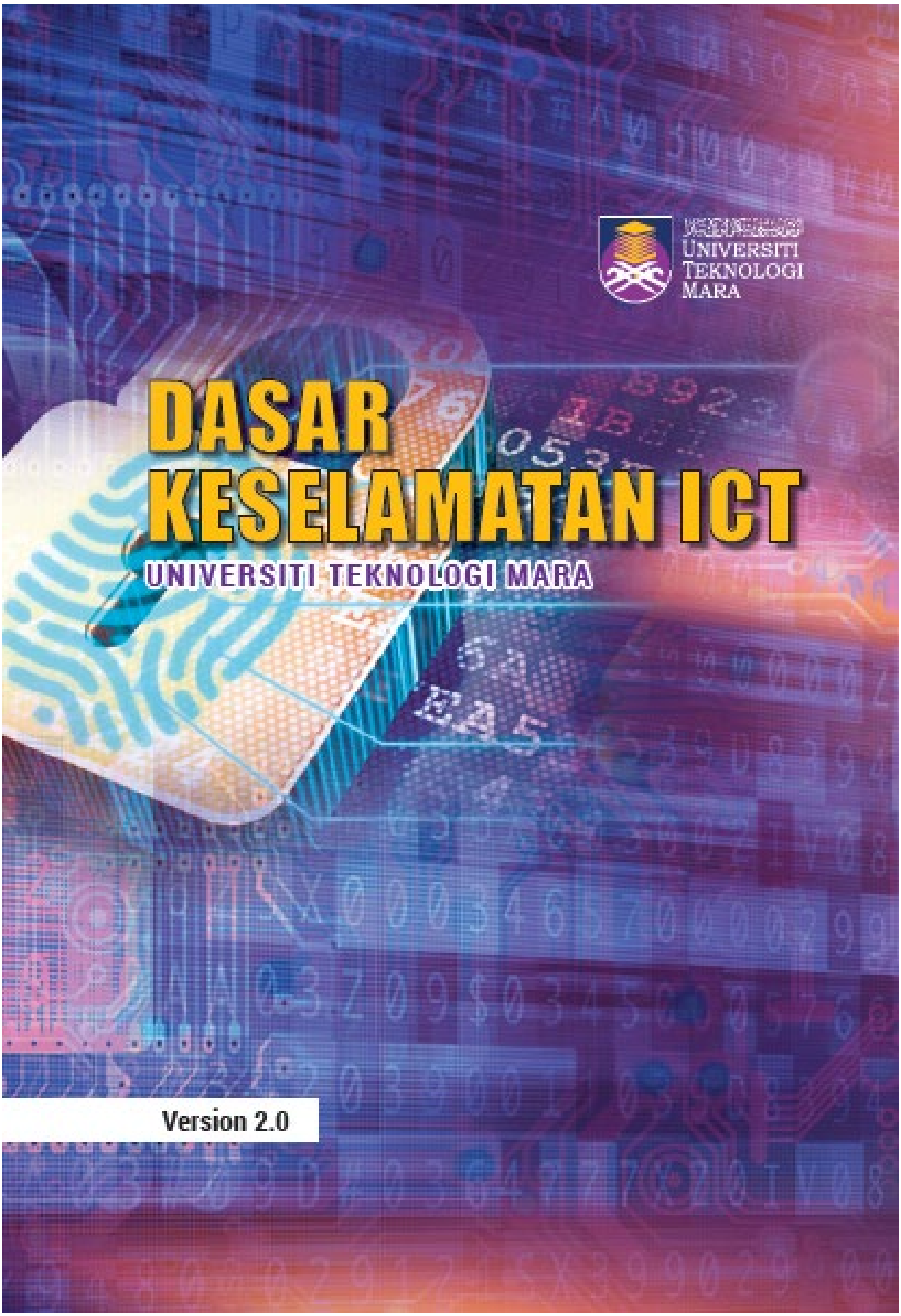

UNIVERSITI
TEKNOLOGI
MARA
DASAR
KESELAMATAN ICT
UNIVERSITI TEKNOLOGI MARA
Version 2.0

UNIVERSITI TEKNOLOGI MARA

DASAR
KESELAMATAN ICT
UNIVERSITI TEKNOLOGI MARA

Version 2.0

Pejabat Infrastruktur dan Infostruktur
Aras 5 & 6, Menara SAAS
Universiti Teknologi MARA
Shah Alam, Selangor

31 Oktober 2018

KANDUNGAN

1. PENGENALAN

Dasar Keselamatan ICT (DKICT) UiTM Versi 2.0 merupakan sebuah dokumen yang menggariskan peraturan penggunaan aset dan kemudahan ICT UiTM dengan cara yang betul. Dasar ini juga menerangkan kepada semua pengguna (warga atau pihak ketiga) di UiTM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UiTM.

1.1 PENYATAAN

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

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

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

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

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

DKICT UiTM v 2.0 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:-

a. Penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;

b. Ancaman yang wujud akibat daripada kelemahan tersebut;

c. Risiko yang mungkin timbul; dan

d. Langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

1.2 OBJEKTIF

DKICT UiTM Versi 2.0 diwujudkan untuk memastikan penggunaan sumber dan aset ICT universiti oleh setiap penguna, dari segi infrastruktur, sistem aplikasi, kemudahan serta data, adalah mengikut peraturan dan undang-undang.

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

Objektif utama Keselamatan ICT UiTM ialah seperti berikut:

a. Memastikan kelancaran operasi UiTM 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 UiTM.

1.3 SKOP

Aset ICT UiTM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. DKICT UiTM v2.0 menetapkan keperluan-keperluan asas berikut:

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

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

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, DKICT UiTM v2.0 ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara yang dinyatakan di dalam Dasar ICT UiTM.

1.4 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT UiTM v2.0 dan perlu dipatuhi adalah seperti berikut :

a. Akses atas dasar "perlu mengetahui"

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

i. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat.

Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

ii. Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

b. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

c. Menentukan maklumat sedia untuk digunakan;

d. Menjaga kerahsiaan kata laluan;

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

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

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

b. Pengasingan

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

c. Pengauditan

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

d. Pematuhan

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

e. Pemulihan

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

f. Saling Bergantungan

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

2. PENILAIAN RISIKO KESELAMATAN ICT

UiTM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan vulnerability yang semakin meningkat hari ini. Justeru itu UiTM perlu mengambil langkahlangkah 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.

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

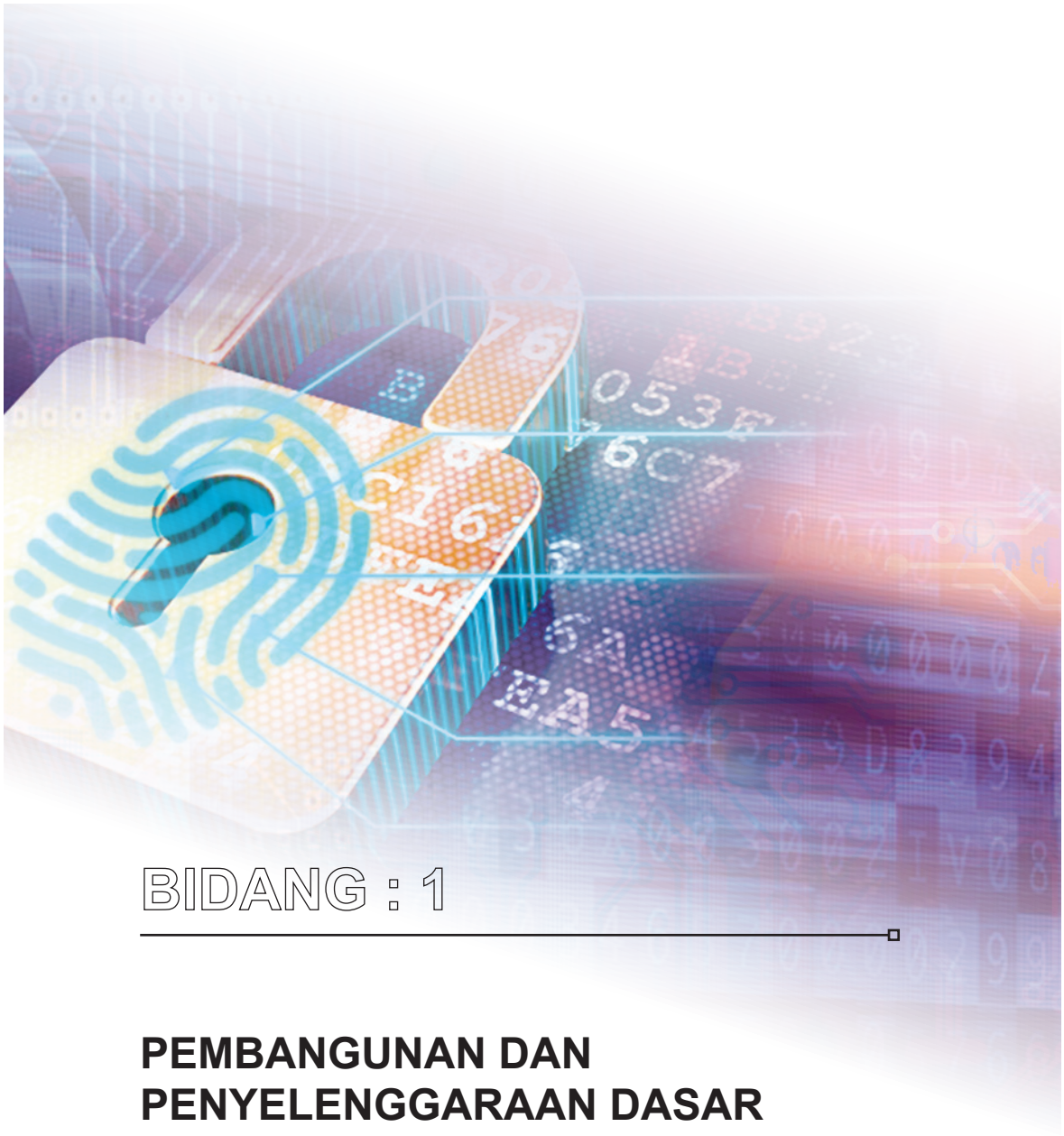
UiTM mengenalpasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b. menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

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

d. memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.



BIDANG : 1

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Bidang 1 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 Dasar Keselamatan ICT

Objektif:

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

1.1.1 Pelaksanaan Dasar

Pelaksanaan dasar ini akan diuruskan oleh jawatankuasa tertinggi ICT Universiti.

1.1.2 Penyebaran Dasar

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

1.1.3 Penyelenggaraan Dasar

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

Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT UiTM:

a. Kenal pasti dan tentukan perubahan yang diperlukan;

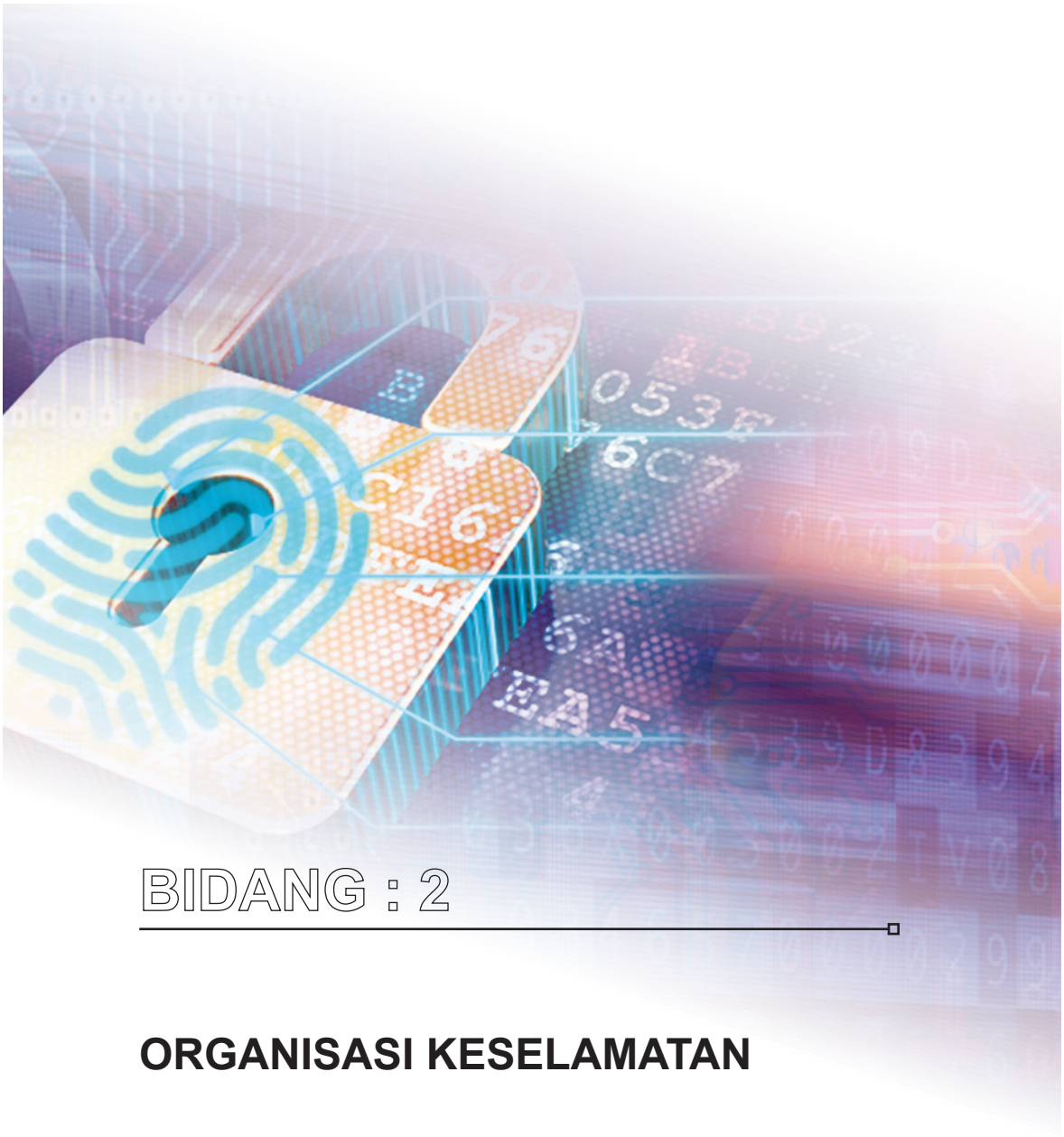
b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan jawatankuasa tertinggi ICT UiTM;

c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh jawatankuasa tertinggi ICT UiTM; dan

d. Dasar ini hendaklah disemak semula sekurang-kurangnya dua tahun sekali atau mengikut keperluan semasa.

1.1.4 Pengecualian Dasar

DKICT UiTM adalah terpakai kepada semua pengguna ICT UiTM termasuk pihak ketiga dan tiada pengecualian diberikan.



BIDANG : 2

ORGANISASI KESELAMATAN

Bidang 2 : **ORGANISASI KESELAMATAN**

2.1 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT UiTM.

2.1.1 Ketua Pegawai Maklumat (CIO)

Timbalan Naib Canselor yang dilantik oleh Pengurusan Tertinggi Universiti merupakan Ketua Pegawai Maklumat (CIO) yang berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut:

a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT UiTM;

b. Memastikan semua pengguna mematuhi DKICT UiTM;

c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;

d. Memastikan pematuhan warga UITM dan pihak ketiga; dan

e. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT UiTM.

2.1.2 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT ialah pegawai yang dilantik bagi memastikan Dasar keselamatan ICT UiTM dipatuhi. Peranan dan tanggungjawab ICTSO dalam perkara-perkara seperti berikut:

a. Merancang, melaksana dan mengurus dan membantu memantau program keselamatan ICT UiTM;

b. Menguatkuasakan Dasar Keselamatan ICT UiTM

c. Memberikan penerangan dan pendedahan berkenaan Dasar Keselamatan ICT UiTM kepada pengguna;

d. Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT UITM;

   i. Melaksanakan pengauditan, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

   ii. Melaporkan insiden keselamatan ICT kepada pengurusan UiTM;

   iii. Bekerjasama dengan semua pihak yang berkaitan dalam menangani ancaman atau insiden keselamatan ICT dan memeperakukan langkah penyelesaian atau pencegahan;

   iv. Merancang penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT UiTM;

   v. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT; dan

   vi. Melaporkan insiden keselamatan ICT kepada CIO dan Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU.

2.1.3 Pengarah Pengurusan ICT UiTM

Peranan dan tanggungjawab Pengarah Pengurusan ICT UiTM adalah seperti berikut:

a. Memantau program keselamatan ICT UiTM yang telah dirangka;

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

c. Memelihara integriti maklumat, menggalak perkongsian maklumat dan menyediakan mekanisme penyebaran maklumat menerusi ICT kepada pengguna-pengguna yang sah di dalam atau luar UiTM.

2.1.4 Pentadbir Sistem ICT

Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara perjalanan dan fungsi sesuatu sistem atau kemudahan ICT.

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang, atau berlaku perubahan dalam bidang tugas.

b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sistem sebagaimana yang telah ditetapkan di dalam DKICT UiTM;

   i. Memantau aktiviti capaian sistem aplikasi pengguna;

   ii. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;

   iii. Menganalisa dan menyimpan rekod jejak audit; dan

   iv. Menyediakan laporan mengenai aktiviti capaian secara berkala.

2.1.5 Pengguna

Pengguna terdiri daripada staf pentadbiran dan akademik, pelajar, pelawat, pelatih, ahli alumni dan mana-mana pihak yang mempunyai ikatan kontrak atau hubungan, sama ada secara bertulis atau tidak, dengan UiTM, yang menggunakan kemudahan ICT universiti.

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a. Membaca, memahami dan mematuhi DKICT UiTM;

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 DKICT UiTM dan menjaga kerahsiaan maklumat UiTM;

e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;

f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan

g. Menandatangani Surat Akuan Pematuhan DKICT UiTM.

2.1.6 Jawatankuasa Keselamatan dan Pengurusan Risiko ICT UiTM

Jawatankuasa Keselamatan dan Pengurusan Risiko ICT UiTM merupakan jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT UiTM (lantikan dari semasa ke semasa).

Bidang kuasa:

a. Merangka dan menyemak semula dokumen DKICT UiTM mengikut keperluan yang termaktub di dalam DKICT UiTM;

b. Memantau tahap pematuhan keselamatan ICT;

c. Memperaku dan menyemak semula garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam UiTM yang mematuhi keperluan DKICT UiTM;

d. Memastikan DKICT UiTM selaras dengan dasar-dasar ICT kerajaan semasa;

e. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa UiTM;

f. Membincang tindakan yang melibatkan pelanggaran DKICT UiTM;

g. Mencadangkan keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden;

h. Mengkaji semula dan mengesyorkan strategi pengurusan risiko bagi Pengurusan ICT, polisi dan toleransi risiko untuk kelulusan pihak pengurusan Pengurusan ICT;

i. Mengkaji semula dan menilai polisi pengurusan risiko dan rangka kerja bagi mengenal pasti risiko ICT Pengurusan ICT,

j. Mengira, memantau dan mengawal risiko serta tahap keberkesanan kegiatan tersebut;

k. Memastikan infrastruktur, sumber dan sistem yang mencukupi tersedia untuk pengurusan risiko berkesan; dan

l. Mengkaji semula laporan berkala pengurusan mengenai pendedahan risiko dan kegiatan pengurusan risiko untuk diserahkan kepada Unit Pengurusan Risiko Universiti.

2.1.7 Pasukan Tindak Balas Insiden Keselamatan ICT UiTM (UiTMCERT)

Keanggotaan UiTMCERT adalah seperti berikut:

Pengarah UiTMCERT : ICTSO

Pengurus UiTMCERT : Ketua Bahagian Keselamatan ICT

Ahli UiTMCERT : staf dari unit/bahagian/jabatan yang dilantik.

Peranan dan tanggungjawab UiTMCERT adalah seperti berikut:

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

b. Merekod dan menjalankan siasatan awal insiden yang diterima;

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

d. Menasihati UiTM mengambil tindakan pemulihan dan pengukuhan;

e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada UiTM.

2.2 Pihak Ketiga

Objektif:

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

2.1.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

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

Perkara yang perlu dipatuhi termasuk yang berikut:

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang, atau berlaku perubahan dalam bidang tugas;

b. Membaca, memahami dan mematuhi DKICT UiTM;

c. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

d. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;

e. Akses kepada aset ICT UiTM perlu berlandaskan kepada perjanjian kontrak;

f. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:-

a. DKICT UiTM;

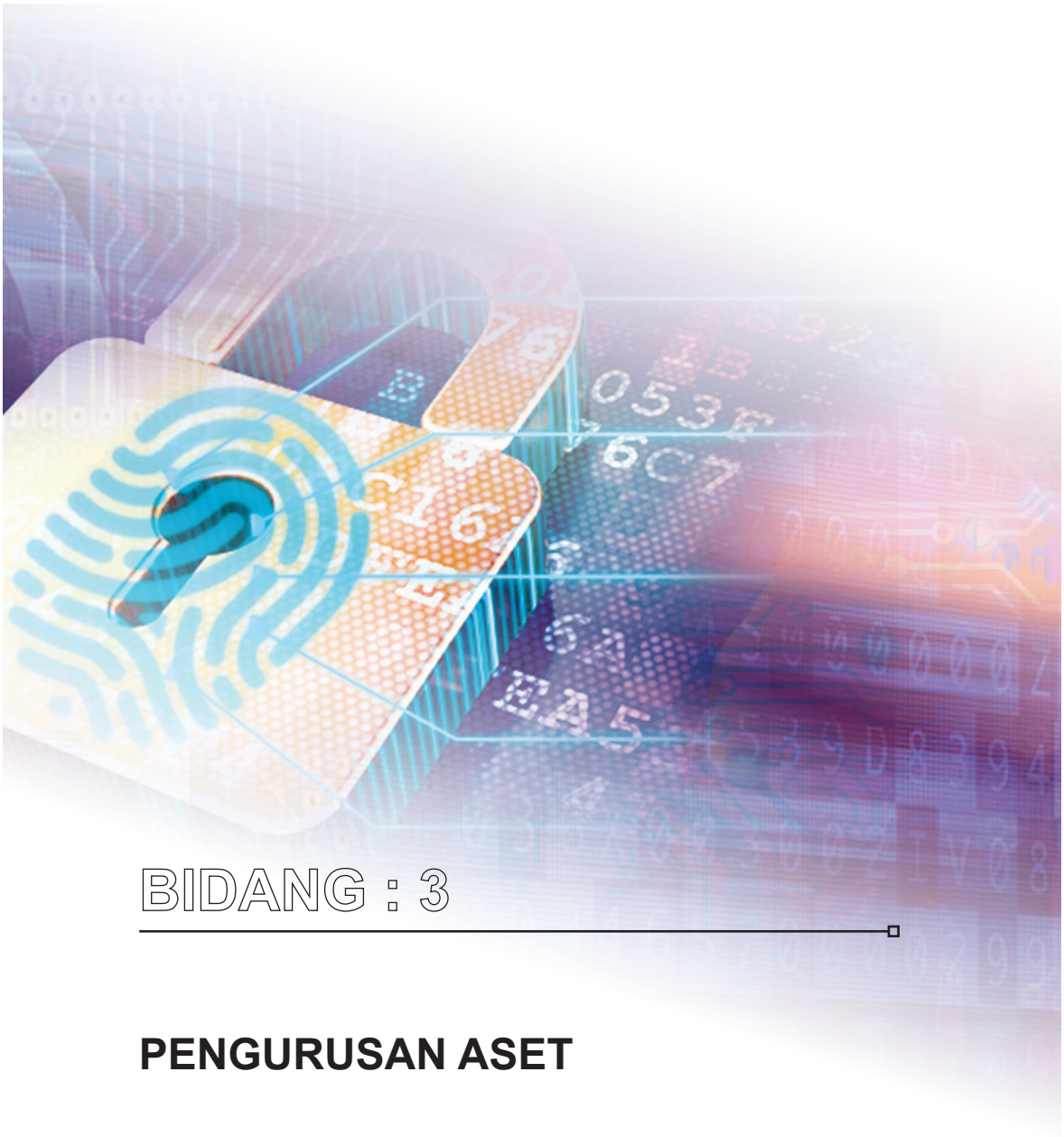
b. Tapisan Keselamatan;

c. Perakuan Akta Rahsia Rasmi 1972;

d. Hak Harta Intelek;

e. Peraturan-peraturan lain yang diguna pakai oleh pihak Universiti; dan

f. Menandatangani Surat Akuan Pematuhan DKICT UiTM.



BIDANG : 3

PENGURUSAN ASET

Bidang 3 : **PENGURUSAN ASET**

3.1 Akauntabiliti Aset

Objektif :

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

3.1.1 Inventori Aset

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

Perkara yang perlu dipatuhi adalah seperti berikut:

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

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

c. Mengenalpasti lokasi semua aset ICT yang telah ditempatkan di UiTM;

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

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

3.2 Pengelasan dan Pengendalian Maklumat

Objektif:

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

3.2.1 Pengelasan Maklumat

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

a. Rahsia Besar;

b. Rahsia;

c. Sulit; atau

d. Terhad.

3.2.2 Pengendalian Maklumat

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

a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

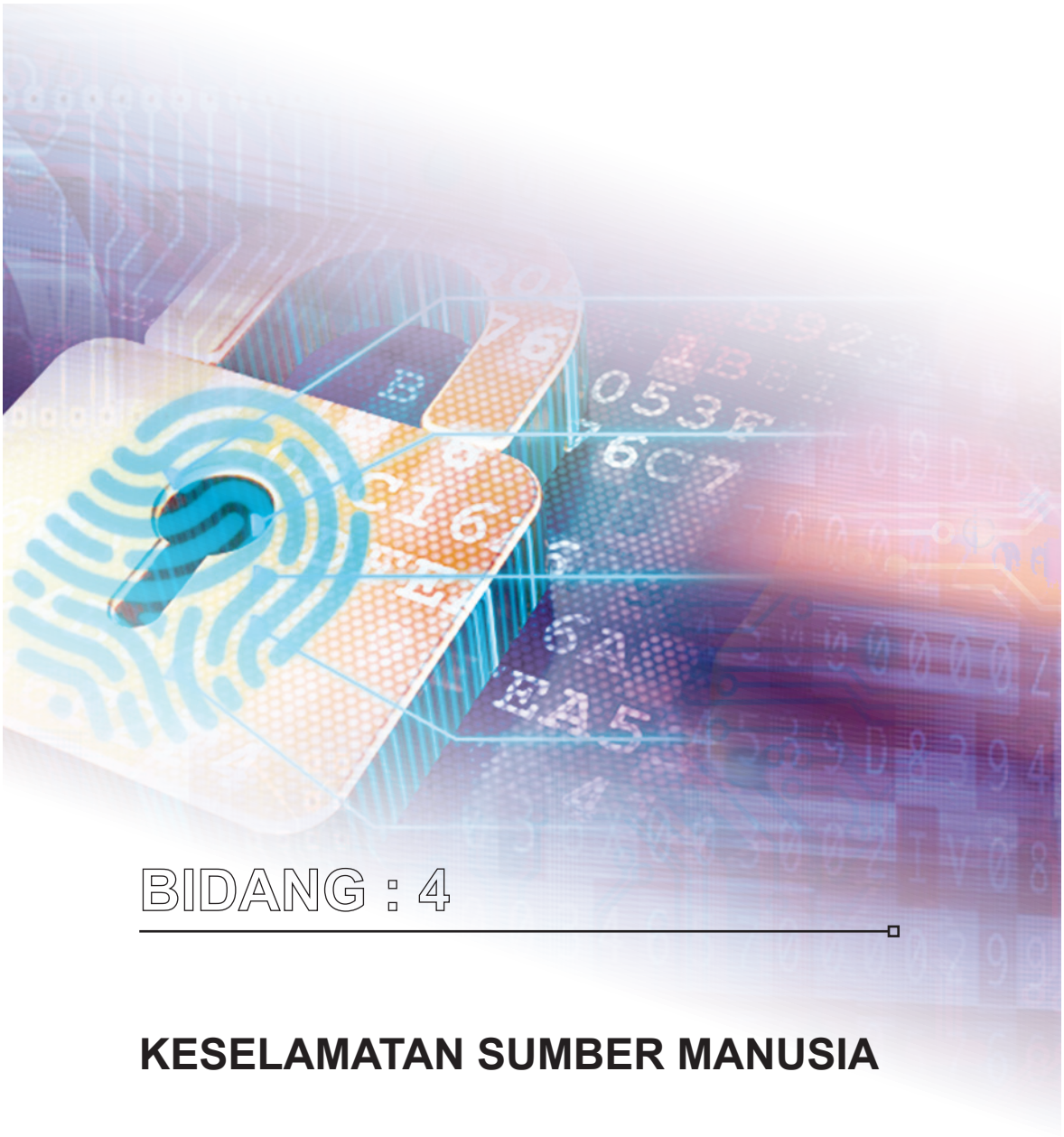
c. Menentukan maklumat sedia untuk digunakan;

d. Menjaga kerahsiaan kata laluan;

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

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

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



BIDANG : 4

KESELAMATAN SUMBER MANUSIA

Bidang 4 : KESELAMATAN SUMBER MANUSIA

4.1 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

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

4.1.1 Sebelum Perkhidmatan

Perkara yang mesti dipatuhi termasuk yang berikut:

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

b. Menjalankan tapisan keselamatan untuk staf UiTM, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan

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

4.1.2 Dalam Perkhidmatan

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

Perkara yang mesti dipatuhi termasuk yang berikut:

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

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

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

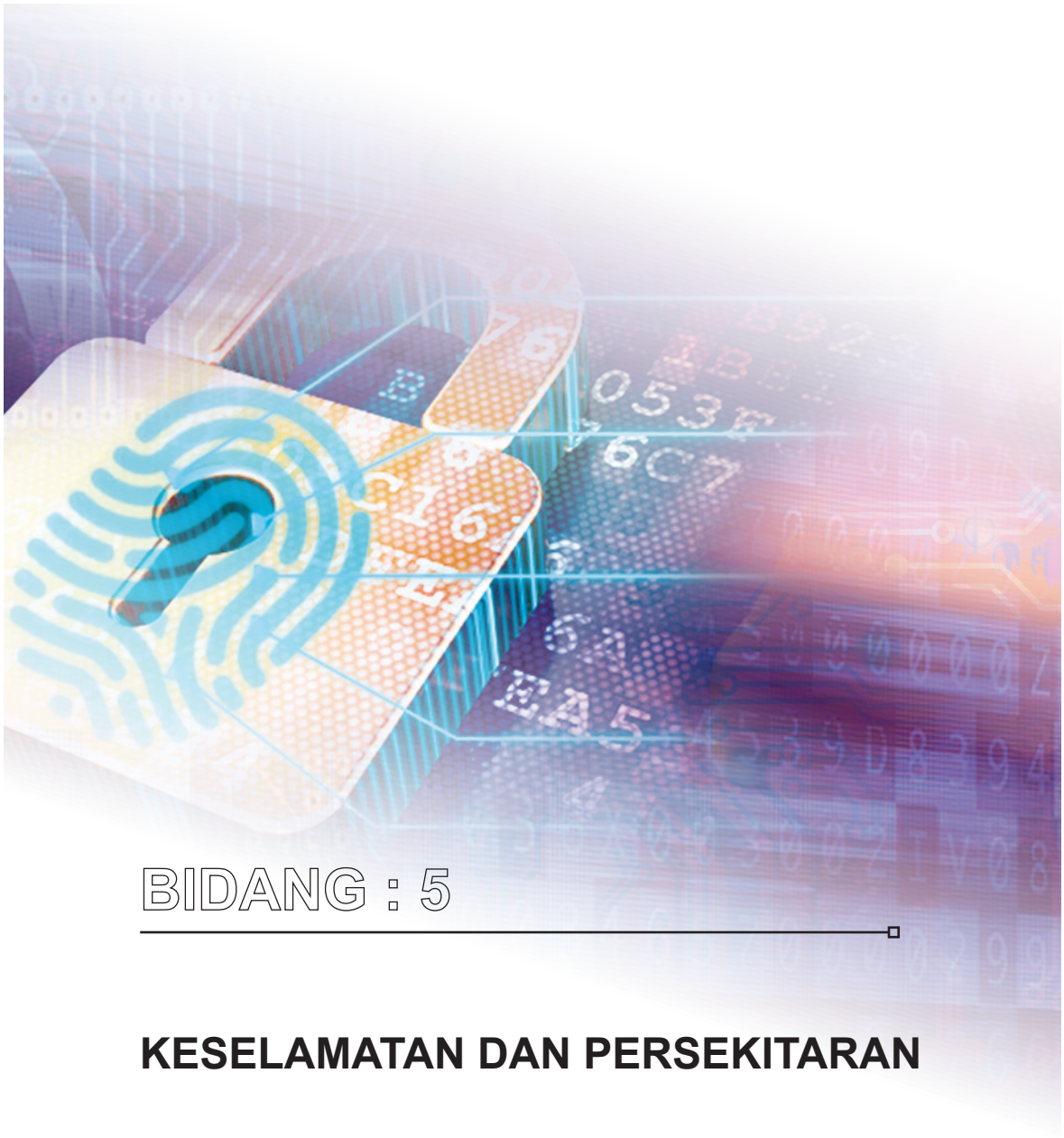
4.1.3 Bertukar Atau Tamat Perkhidmatan

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

Perkara yang perlu dipatuhi termasuk:

a. Memastikan semua aset ICT dikembalikan kepada PTJ mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

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



BIDANG : 5

KESELAMATAN DAN PERSEKITARAN

Bidang 5 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

5.1 Keselamatan Kawasan

Objektif :

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

5.1.1 Kawalan Kawasan

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

Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:

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

b. Akses adalah terhad kepada warga UiTM yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

c. Akses ke Pusat Data/Pusat Pemulihan Bencana Universiti/Bilik Server terhad kepada staf operasi pengurusan Pusat Data/Pusat Pemulihan Bencana/ Pusat Pemulihan Bencana/Bilik Server dan staf tertentu sahaja (Mempunyai keperluan akses ke Pusat Data/Pusat Pemulihan Bencana/Bilik Server secara kerap dan telah pun mendapat kebenaran dari Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana/ Ketua Bahagian Pengurusan Sistem/ Pengarah

Pengurusan ICT/Ketua ICT PTJ);

d. Pihak ketiga yang memerlukan akses ke Pusat Data/Pusat Pemulihan Bencana/Bilik Server untuk melaksanakan kerja–kerja penyelenggaraaan perlulah diiringi oleh Staf Operasi Pusat Data/Pusat Pemulihan Bencana/Ketua ICT PTJ;

e. Lawatan dari mana-mana agensi luar/Pelajar ke Pusat Data/Pusat Pemulihan Bencana/Bilik Server perlulah terlebih dahulu membuat permohonan rasmi melalui surat dengan menyatakan tujuan lawatan kepada Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana/ Ketua Pengurusan Sistem/ Pengarah Pengurusan ICT/ Ketua ICT PTJ;

f. Dalam keadaan kecemasan, kebenaran akses ke Pusat Data/Pusat Pemulihan Bencana/Bilik Server oleh staf akan diberikan dan dikoordinasikan oleh Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana/ Ketua ICT PTJ bertanggungjawab tanpa mengira waktu dan masa. Apabila terdapat keperluan untuk membuka pintu Pusat Data/Pusat Pemulihan Bencana/ Bilik Server yang disebabkan oleh kecemasan, Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana/ Ketua ICT PTJ yang bertanggungjawab perlu:-

   i. Mengesahkan situasi kecemasan yang berlaku

   ii. Mengesahkan dan mengenalpasti individu yang memohon akses dan kaitan dalam menyelesaikan masalah kecemasan tersebut (e.g. *police responding to a bomb threat, firefighters responding to a fire alarm, HVAC personnel responding to a temperature alarm,* etc.);

   iii. Merekodkan maklumat (tarikh, masa, nama , sebab dan sebagainya)

   iv. Makluman berkaitan dengan insiden perlulah dilaporkan kepada Ketua Polis bantuan UiTM dan Pengarah Pengurusan ICT/Ketua PTJ.

e. Pemantauan dibuat menggunakan *Access Door* melalui Kad Pintar Staf atau lain-lain peralatan yang sesuai;

f. Peralatan *Access Door* dan *Log akses* perlu diperiksa secara berjadual;

g. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam;

h. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;

i. Memperkukuh dinding dan siling;

j. Menghadkan jalan keluar masuk;

k. Mengadakan kaunter kawalan; dan

l. Menyediakan tempat atau bilik khas untuk pelawat

5.1.2 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a. Warga UiTM:-

   i. Semua warga UiTM hendaklah memakai atau mengenakan kad pintar UiTM sepanjang waktu berada di dalam kampus; dan

   ii. Semua kad pintar UiTM hendaklah diserahkan kembali kepada UiTM apabila berhenti/ tamat atau bersara.

a. Pelawat

b. Setiap pelawat perlu mendaftar dan mendapatkan Pas Pelawat di pintu masuk ke kawasan atau tempat berurusan dan pas ini hendaklah dikembalikan semula selepas tamat lawatan. Kehilangan pas mestilah dilaporkan dengan segera.

5.1.3 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pengguna UiTM yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan ICT di UiTM adalah pusat data, pusat pemulihan bencana, bilik server, bilik rangkaian dan lain-lain kawasan yang diwartakan sebagai kawasan larangan.

a. Akses kepada kawasan larangan hanyalah kepada pengguna UiTM yang dibenarkan sahaja;

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

5.2 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT UiTM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

5.2.1 Peralatan ICT

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

c. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pengurusan ICT;

d. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pengurusan ICT untuk di baik pulih;

e. Pengguna mesti memastikan perisian antivirus bagi semua peralatan ICT yang dibekalkan oleh Pengurusan ICT seperti komputer peribadi, komputer riba dan server yang berada di bawah tanggungjawab mereka sentiasa aktif (*activated*) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan;

f. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pengurusan ICT;

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

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

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

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

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

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

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

n. Peralatan ICT yang hendak dibawa keluar dari premis UiTM, perlulah mendapat kelulusan Pengarah Pengurusan ICT/PTJ/Ketua ICT PTJ yang berkenaan bagi tujuan pemantauan;

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

p. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat; dan

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

5.2.2 Media Storan

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

Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil:

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

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

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

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

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

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

g. Akses dan pergerakan media storan perlu direkodkan;

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

i. Sebarang kehilangan media storan yang berlaku hendaklah dilaporkan kepada PTJ masing-masing.

5.2.3 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan

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

5.2.4 Media Perisian Dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan UiTM;

b. Sistem aplikasi dalaman tidak dibenarkan dibentangkan atau diagih kepada pihak lain kecuali dengan kebenaran Pengarah Pengurusan ICT atau PTJ;

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.

5.2.5 Penyelenggaraan Perkakasan

Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.

Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

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

b. Memastikan perkakasan hanya diselenggara oleh staf atau pihak yang dibenarkan sahaja;

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

d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

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

5.2.6 Peralatan di Luar Premis

Perkakasan yang dibawa keluar dari premis UiTM adalah terdedah kepada pelbagai risiko.

Perkakasan yang dibawa keluar premis UiTM merangkumi:

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Peralatan perlu dilindungi dan dikawal sepanjang masa;

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

c. Mendapatkan kelulusan mengikut peraturan sedia ada UiTM bagi membawa keluar peralatan tertakluk kepada tujuan yang dibenarkan; dan

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

5.2.7 Pelupusan Perkakasan

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada aset tetap atau inventori yang dibekalkan oleh UiTM dan ditempatkan di UiTM. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa.

Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan UiTM:

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

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

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

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

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

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

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

h. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:

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

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

   iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di UiTM;

   iv. Memindah keluar dari UiTM mana-mana peralatan ICT yang hendak dilupuskan; dan

   v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab UiTM.

f. Proses pelupusan mestilah mengikut Peraturan atau Pekeliling terkini yang dikeluarkan oleh Pejabat Bendahari UiTM; dan

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

5.3 Keselamatan Persekitaran

Objektif :

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

5.3.1 Kawalan Persekitaran

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

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

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

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

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

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

e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari asset ICT;

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

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

h. Mengadakan penyenggaraan berkala; dan

i. Menggunakan vakum yang memenuhi piawai untuk membersihkan peralatan.

5.3.2 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

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

5.3.3 Kabel Data

Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :

a. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan;

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

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

d. Melabelkan kabel menggunakan kod dan label yang mengikut piawaian; dan

e. Bilik server/rangkaian hendaklah sentiasa berkunci dan hanya boleh dicapai oleh staf yang dibenarkan.

5.3.4 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan oleh Unit Pengurusan Risiko UiTM;

b. Melaporkan insiden kecemasan kepada Polis Bantuan di Pejabat Polis Bantuan UiTM;

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

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

5.4 Keselamatan Dokumen

Objektif :

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

5.4.1 Dokumen

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

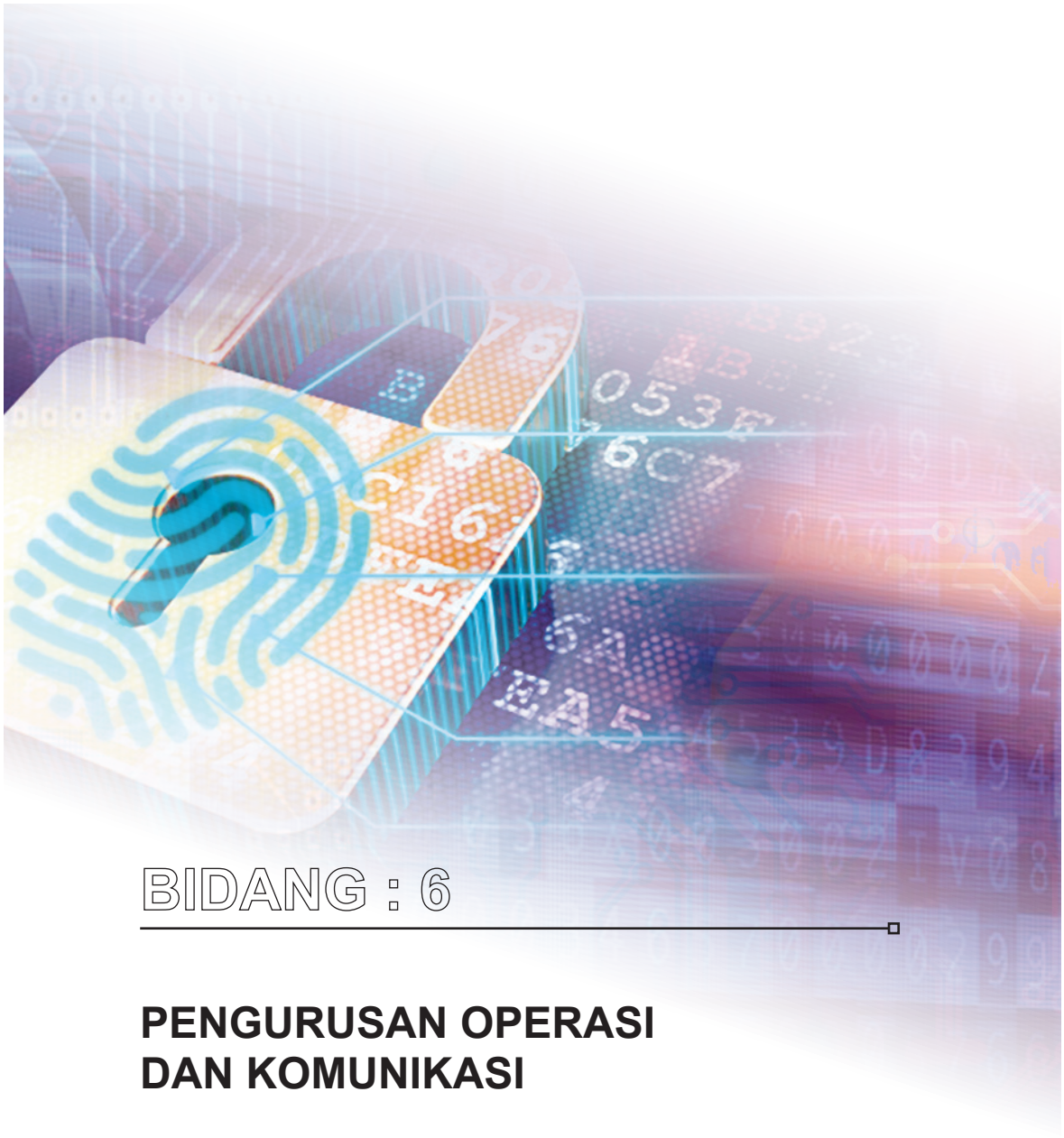
a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;

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

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

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

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



BIDANG : 6

PENGURUSAN OPERASI DAN KOMUNIKASI

Bidang 6 : PENGURUSAN OPERASI DAN KOMUNIKASI

6.1 Pengurusan Prosedur Operasi

Objektif :

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

6.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

6.1.2 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada PTJ atau pemilik aset ICT terlebih dahulu;

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

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

d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat samada secara sengaja atau pun tidak.

6.1.3 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

6.2 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.

6.2.1 Perkhidmatan Penyampaian

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

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

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

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

6.3 Perancangan dan Penerimaan Sistem

Objektif :

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

6.3.1 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

6.3.2 Penerimaan Sistem

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

6.4 Perisian Berbahaya

Objektif :

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

6.4.1 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

d. Mengemaskini anti virus dengan *pattern* antivirus yang terkini;

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

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

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

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

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

6.4.2 Perlindungan dari *Mobile Code*

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

6.5 *Housekeeping*

Objektif :

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

6.5.1 *Backup*

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Membuat *backup* ke atas semua sistem perisian dan aplikasi secara berjadual;

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

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

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

e. Media *backup* dan prosedur *restore* diuji untuk *test verification* sekali (1) setahun

6.6 Pengurusan Rangkaian

Objektif :

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

6.6.1 Kawalan Infrastruktur Rangkaian

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

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

e. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Ketua Pengurusan Rangkaian;

f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan UiTM;

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

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

i. Sebarang penyambungan rangkaian yang bukan di bawah kawalan UiTM adalah tidak dibenarkan;

j. Semua pengguna hanya dibenarkan menggunakan rangkaian UiTM sahaja dan penggunaan modem asing adalah dilarang sama sekali; dan

k. Kemudahan bagi *wireless* LAN mesti mempunyai kawalan keselamatan.

6.7 Pengurusan Media

Objektif :

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

6.7.1 Penghantaran dan Pemindahan

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

6.7.2 Prosedur Pengendalian Media

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

a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

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

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

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

e. Menyimpan semua media di tempat yang selamat; dan

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

6.7.3 Keselamatan Sistem Dokumentasi

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

a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;

b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan

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

6.8 Pengurusan Pertukaran Maklumat

Objektif :

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

6.8.1 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. 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 UiTM dengan agensi luar;

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

d. Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya.

6.9 Pengurusan Mel Elektronik (E-mel)

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

6.9.1 Penggunaan Am

Pengguna e-mel perlu mematuhi perkara-perkara berikut:

a. Perisian-perisian berlesen dan mempunyai hakmilik terpelihara atau intelek tidak boleh disebarkan melalui e-mel individu atau organisasi;

b. Aktiviti *spamming* atau *mail-bombing* dan penyebaran e-mel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman dan gangguan) kepada individu, *mailing list* atau *discussion groups* sama ada di dalam rangkaian setempat (LAN) UiTM atau ke rangkaian luas (WAN) dan Internet oleh pengguna adalah tidak dibenarkan;

c. UiTM berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel dan virus (*email filter* dan *anti virus*) yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis menyekat atau menghapuskan mana-mana *e-mel* yang disyaki mengandungi virus atau berunsur *Spamming* daripada memasuki ke dalam server, stesen kerja atau rangkaian setempat (LAN) UiTM dan keluar daripada server, stesen kerja atau rangkaian setempat (LAN) UiTM.

d. UiTM tidak bertanggungjawab secara langsung atau tidak langsung terhadap pengguna yang menjadi penghantar (*sender*) atau penerima (*receiver*) kepada sebarang e-mel yang berunsur *spamming* atau penyebaran e-mel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman dan gangguan) sama ada secara disedari/sengaja atau tidak disedari/ sengaja olehnya; dan

a. UiTM tidak bertanggungjawab secara langsung atau tidak langsung terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, data, kotak e-mel atau fail yang disimpan oleh pengguna di dalam stesen kerja atau server akibat daripada penggunaan perkhidmatan e-mel;

b. Untuk keselamatan penggunaan, perkara berikut perlu diberi perhatian oleh pengguna:

   i. Tukar kata laluan secara berkala (dicadangkan setiap 12 bulan) bagi mengelakkan akaun e-mel diceroboh;

   ii. Tidak berkongsi kata laluan dengan pengguna lain dan tidak melayan mana-mana permintaan untuk mendapat kata laluan;

   iii. Berhati-hati ketika menerima fail kepilan (*attachments*). Fail kepilan mungkin mengandungi *letterbombs* atau virus yang boleh merosakkan komputer dan rangkaian UiTM. Fail kepilan yang sering mengandungi virus ialah fail yang mempunyai *extension* '.exe', '.zip', 'pif', '.scr' dan sebagainya;

   iv. *Log out* setelah selesai sesi penggunaan e-mel bagi menyelamatkan akaun dari pencerobohan atau tutup *browser* yang digunakan setelah sesi capaian e-mel selesai; dan

   v. Tidak menjawab e-mel yang tidak berkenaan (seperti *spam*, ugutan atau ofensif) kerana dengan menjawab e-mel yang sedemikian, pengguna mendedahkan diri kepada aktiviti yang tidak bertanggungjawab. Pengguna bertanggungjawab melapor penerimaan e-mel sedemikian kepada pentadbir e-mel Pengurusan ICT dan PTJ.

6.9.2 Penggunaan Khusus

a. Alamat e-mel yang diberikan oleh UiTM kepada pengguna individu atau jabatan/persatuan adalah muktamad dan ditentukan oleh UiTM. Pengguna tidak dibenarkan untuk memohon penukaran alamat e-mel;

b. Pengguna diberikan ruangan storan e-mel 1 GB sahaja;

c. Seseorang pengguna individu tidak dibenarkan untuk memohon dan memiliki lebih dari satu akaun atau alamat e-mel UiTM pada satu-satu masa;

d. Setiap alamat e-mel yang disediakan adalah untuk kegunaan individu atau jabatan/persatuan berkenaan sahaja. Ia tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran;

e. Pengguna dilarang menggunakan kemudahan e-mel untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan dan undang-undang UiTM dan negara;

f. Semua pengguna yang diberi kemudahan e-mel UiTM tidak dibenarkan mengguna e-mel luar (seperti *hotmail, yahoo* dan lain-lain) untuk tujuan rasmi. Pentadbir Rangkaian berhak menghalang penggunaan e-mel tersebut jika didapati memudarat dan membebankan rangkaian UiTM;

g. Di dalam kes sistem tergendala (rosak), pihak pentadbir mel hanya bertanggungjawab untuk memulihkan kembali (*restore*) maklumat akaun pengguna dan bukannya kandungan/kotak e-mel (*mailbox*) pengguna;

h. Atas keperluan audit, keselamatan dan penggunaan, pentadbir e-mel berhak memeriksa dan melihat isi kandungan e-mel dan ruang storan pengguna-pengguna; dan

i. Pengguna bertanggungjawab sepenuhnya di atas penggunaan perisian e-mel.

6.9.3 Permohonan

Permohonan untuk mendapatkan kemudahan e-mel boleh dibuat oleh staf UiTM dengan cara mengisi Borang Permohonan e-mel Individu atau secara elektronik. Manakala jabatan dan persatuan rasmi UiTM boleh memohon kemudahan e-mel dengan cara mengisi Borang Pemohonan E-Mel Jabatan & Persatuan iaitu yang boleh diperolehi di PTJ/Kampus Negeri atau melalui laman web rasmi UiTM. Borang yang telah lengkap diisi hendaklah dimajukan kepada PTJ/Kampus Negeri.

Permohonan yang telah diluluskan akan dikembalikan kepada pemohon dengan disertakan maklumat alamat e-mel dan kata laluan.

6.9.4 Penamatan Kemudahan

UiTM boleh menamatkan kemudahan akaun e-mel yang telah diberikan kepada staf dan pelajar atas sebab-sebab berikut:-

a. Staf telah tamat atau ditamatkan perkhidmatan dengan UiTM secara rasmi;

b. Pelajar telah tamat atau ditamatkan pengajiannya di UiTM secara rasmi;

c. Jabatan atau Persatuan yang telah dibubar secara rasmi oleh pihak pengurusan UiTM;

d. Permintaan dari staf atau pelajar sendiri untuk menamatkan perkhidmatan tersebut; dan

e. Staf atau pelajar yang tidak bersetuju atau melanggar syarat-syarat di dalam Garis Panduan Pengurusan ICT Universiti.

6.10 Pengurusan Perkhidmatan Server (Pelayan)

Seksyen ini menerangkan peraturan dan perkara yang perlu dipatuhi untuk pengoperasian server untuk memastikan server tersebut diselenggara dan dipasang dengan sedemikian rupa untuk mengelakkan daripada ia dicerobohi atau dicapai oleh individu yang tidak sepatutnya.

6.10.1 Hak Milik

Semua server yang diperoleh mengikut tatacara perolehan atau sumbangan daripada mana-mana pihak adalah menjadi hak milik UiTM sepenuhnya.

6.10.2 Tanggungjawab

Semua PTJ/Kampus Negeri yang membuat pembelian server adalah bertanggungjawab sepenuhnya kepada server tersebut. Tanggungjawab ini boleh dipecahkan kepada:

a. Pemilik

Pemilik adalah PTJ yang membuat perolehan kepada sesuatu server. Pemilik adalah bertanggungjawab bagi memastikan server di bawah pengawasannya berada di dalam keadaan baik. Setiap PTJ dinasihatkan agar melantik seorang staf yang mempunyai kemahiran teknikal yang berkaitan bagi menguruskan server yang dimilikinya. Pengurusan server oleh PTJ adalah tertakluk kepada Dasar Keselamatan ICT UiTM serta undang-undang yang dikuatkuasakan dari semasa ke semasa; dan

b. Pentadbir Sistem

Pentadbir Sistem bertanggungjawab memastikan server diurus dan ditadbir dengan betul serta memenuhi keperluan pemilik *server* dan dasar yang dilaksanakan. Pentadbir adalah bertanggungjawab sepenuhnya ke atas keselamatan data dan sistem di dalam *server*.

6.10.3 Penyataan

Setiap PTJ atau penyedia server perlu mematuhi peraturan-peraturan berikut:

a. Pentadbir sistem perlu memastikan keselamatan server daripada pencerobohan. Ini termasuk tetapi tidak terhad kepada membuat pemeriksaan ke atas proses tersembunyi (*hidden processes*), *daemons*, mengemaskini perisian seperti e-mel dan laman web, dan mengenal pasti pengguna-pengguna. Jabatan atau penyedia server boleh menyedia *firewall* khusus untuk tujuan ini;

b. Pentadbir sistem perlu mengenal pasti tahap capaian pengguna dan penggunaan server secara jelas. Ini akan menghasilkan capaian yang lebih terkawal;

c. Server yang melibatkan penyimpanan maklumat yang penting dan kritikal perlu mempunyai *backup* yang lengkap untuk mengelak kehilangan maklumat dan mengurangkan masa *downtime.* Urusan operasi *backup* adalah di bawah tanggung jawab Pengurusan Pusat Data/Pusat Pemulihan Bencana/Bilik Server dan Pentadbir sistem;

d. Server yang digunakan untuk projek pelajar perlu mendapat kelulusan daripada penyelia projek / Dekan. Alamat IP dalaman statik digunakan untuk server ini. Alamat IP global boleh diberi kepada projek yang memerlukan capaian Internet; dan

e. Semua Pentadbir sistem yang dipertanggungjawabkan perlu mematuhi peraturan berikut:

    i. Pertukaran alamat IP tidak dibenarkan sama sekali tanpa kebenaran Pentadbir Alamat IP;

    ii. Login dan kata laluan untuk *root* dan *super-user* adalah di bawah kawalan dan tanggungjawab Pentadbir Sistem dan Pusat Data/Pusat Pemulihan Bencana; dan

    iii. Pentadbir Sistem di Jabatan bertanggungjawab memastikan server tidak disalah guna untuk tujuan yang bukan sepatutnya.

6.10.4 Pengurusan Kata Laluan Server

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

Dalam apa jua keadaan dan sebab, kata laluan bagi peralatan ICT UiTM hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; walaubagaimanapun, bagi kata laluan untuk server, ianya akan disimpan di dalam peti besi dan hanya boleh dicapai oleh tiga orang yang disenaraikan apabila diperlukan.

Pegawai yang disenaraikan adalah :-

a. Pengarah Pengurusan ICT; atau

b. Ketua ICT PTJ; atau

c. Ketua Bahagian Pengurusan Sistem, Jabatan Infostruktur; atau

d. Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana

6.10.5 Permohonan Penempatan Server Di Pusat Data/Pusat Pemulihan Bencana Universiti

Setiap server yang ingin diletakkan di Pusat Data/Pusat Pemulihan Bencana perlu mendapat kelulusan Ketua Pengurusan Pusat Data/Pusat Pemulihan Bencana dengan mengisi borang yang disediakan oleh Pengurusan Pusat Data/Pusat Pemulihan Bencana. Pembekal / Pegawai TanggungJawab diminta menyediakan beberapa perkara iaitu:

a. Railing Kit

b. Power Cord (C13 atau C19)

c. KVM Conventer

d. Salinan Borang Harta Benda KEW312

e. Pegawai yang dihubungi jika berlaku kecemasan

6.10.6 Pelanggaran Prinsip Utama

Sebarang pelanggaran prinsip utama yang berlaku boleh mengakibatkan salah satu daripada perkara-perkara berikut bergantung kepada tahap masalah tersebut:

a. Bagi masalah keselamatan, server akan ditutup sementara sehingga tahap keselamatan server ditingkatkan ke tahap yang sewajarnya;

b. Penyambungan server ke rangkaian akan ditutup;

c. Penutupan operasi server; dan

d. Peringatan kepada pentadbir atau pemilik akan dikeluarkan jika didapati server digunakan untuk aktiviti yang bukan berkaitan urusan rasmi Universiti.

6.11 Pemantauan

Objektif :

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

6.11.1 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:

a. Sebarang percubaan pencerobohan kepada sistem ICT UiTM yang dilaporkan;

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*) yang dilaporkan;

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

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

e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

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

g. Aktiviti penyalahgunaan akaun e-mel; dan

h. Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.

6.11.2 Jejak Audit

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

a. Rekod setiap aktiviti transaksi;

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

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

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

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

Pentadbir Sistem ICT 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.

6.11.3 Sistem Log

Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:

a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

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

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

6.11.4 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

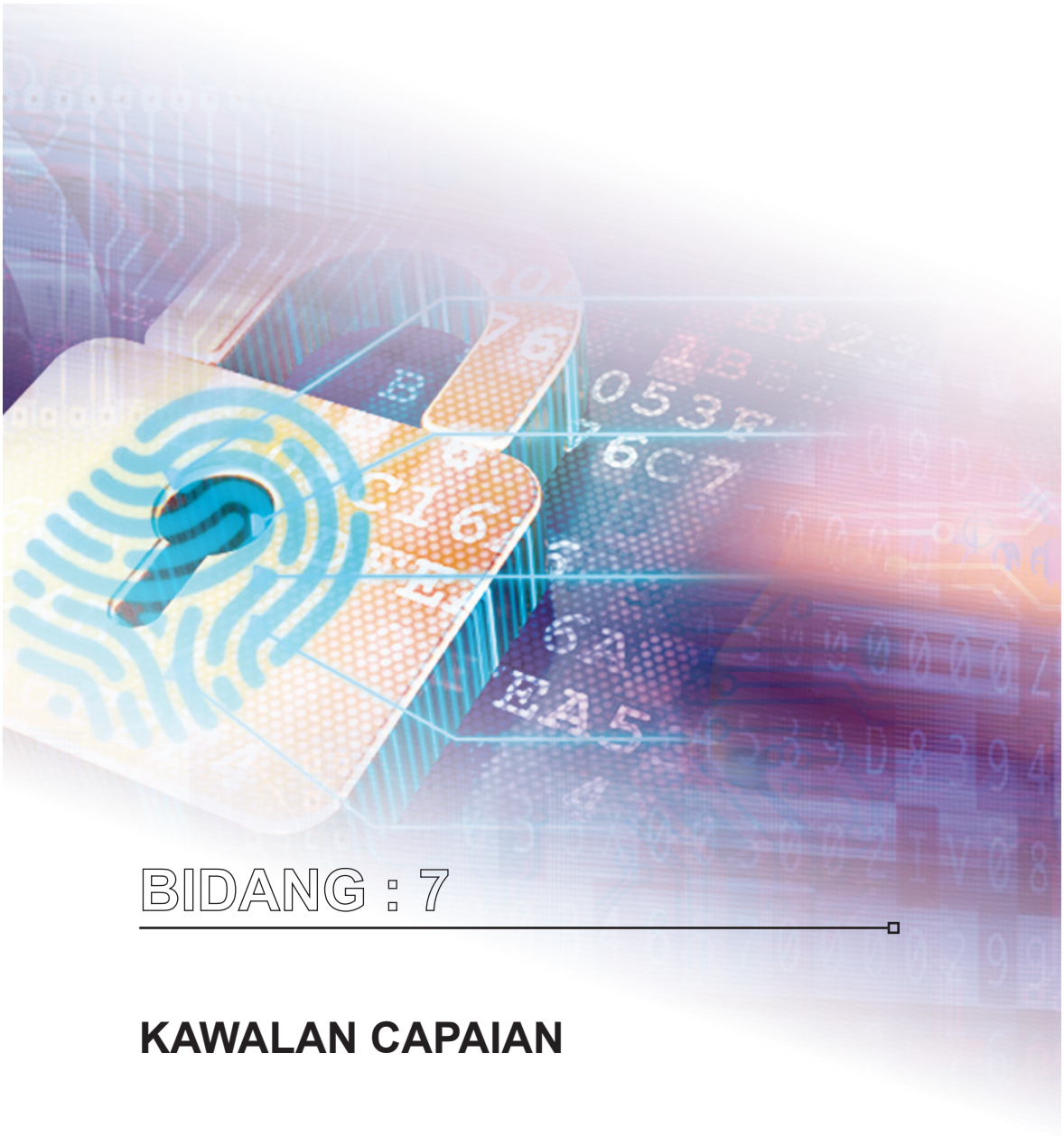
b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;

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

d. Aktiviti pentadbiran dan operator sistem perlu direkodkan;

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

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



BIDANG : 7

KAWALAN CAPAIAN

Bidang 7 : **KAWALAN CAPAIAN**

7.1 Dasar Kawalan Capaian

Objektif :

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

7.1.1 Keperluan Kawalan Capaian

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

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

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

d. Kawalan ke atas kemudahan pemprosesan maklumat.

7.2 Pengurusan Capaian Pengguna

Objektif :

Mengawal capaian pengguna ke atas aset ICT UiTM.

7.2.1 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:

a. Akaun yang diperuntukkan oleh UiTM sahaja boleh digunakan;

b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

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

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

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

f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebabsebab berikut:

   i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi enam (6) bulan;

   ii. Bertukar bidang tugas kerja;

   iii. Bertukar ke agensi lain;

   iv. Bersara; atau

   v. Ditamatkan perkhidmatan.

7.2.2 Hak Capaian

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

7.2.3 Pengurusan Kata Laluan

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

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

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

c. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

d. Kata laluan hendaklah TIDAK dipaparkan semasa input, dalam laporan atau media lain;

e. Kuatkuasakan pertukaran kata laluan semasa log in kali pertama atau selepas log in kali pertama atau selepas kata laluan diset semula;

f. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

g. Kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan;

h. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna;

i. Staf hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

j. Panjang kata laluan mestilah di antara 8-16 aksara dengan gabungan aksara, angka dan aksara khusus;

k. kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

l. had masa *idle* selama 15 minit dan selepas had itu, sesi ditamatkan; dan

m. kata laluan hendaklah ditukar selepas 12 bulan.

7.2.4 *Clear Desk* dan *Clear Screen*

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah samada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-

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

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

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

7.3 Kawalan Capaian Rangkaian

Objektif :

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

7.3.1 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

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

b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna yang menepati kesesuaian penggunaannya;

c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

d. Mengawal capaian fizikal dan logikal ke atas kemudahan *port diagnostic* dan konfigurasi jarak jauh;

e. Mengasingkan capaian mengikut pengguna dan sistem maklumat dalam rangkaian; dan

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

7.3.2 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Penggunaan Internet di UiTM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian UiTM;

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

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

d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja;

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

f. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada PTJ sebelum dimuat naik ke Internet;

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

h. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh UiTM;

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

j. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali tanpa kelulusan Pengarah Pengurusan ICT; dan

k. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:

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

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

7.4 Kawalan Capaian Sistem Pengoperasian

Objektif :

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

7.4.1 Capaian Sistem Pengoperasian

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

Kemudahan ini juga perlu bagi:

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

b. Merekodkan capaian yang berjaya dan gagal;

c. Membekalkan kemudahan untuk pengesahan (bagi sistem kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan); dan kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;

ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian; dan

iii. Menyediakan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

a. Mengawal capaian ke atas sistem operasi menggunakan prosedur log in yang terjamin;

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

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

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

e. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi;

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

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

7.4.2 Kad Pintar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

c. Sebarang kehilangan dan kerosakan perlu dilaporkan kepada Polis Bantuan, UiTM.

7.5 Kawalan Capaian Aplikasi Dan Maklumat

Objektif :

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

7.5.1 Capaian Aplikasi Dan Maklumat

Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di UiTM adalah terhad kepada pengguna dan tujuan yang dibenarkan.

Bagi memastikan kawalan capaian sistem dan aplikasi adalah selamat, langkah-langkah berikut perlu dipatuhi:

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

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

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

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

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

f. *Session timeout* hendaklah dilaksanakan.

7.6 Peralatan Mudah Alih

Objektif :

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

7.6.1 Peralatan Mudah Alih

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

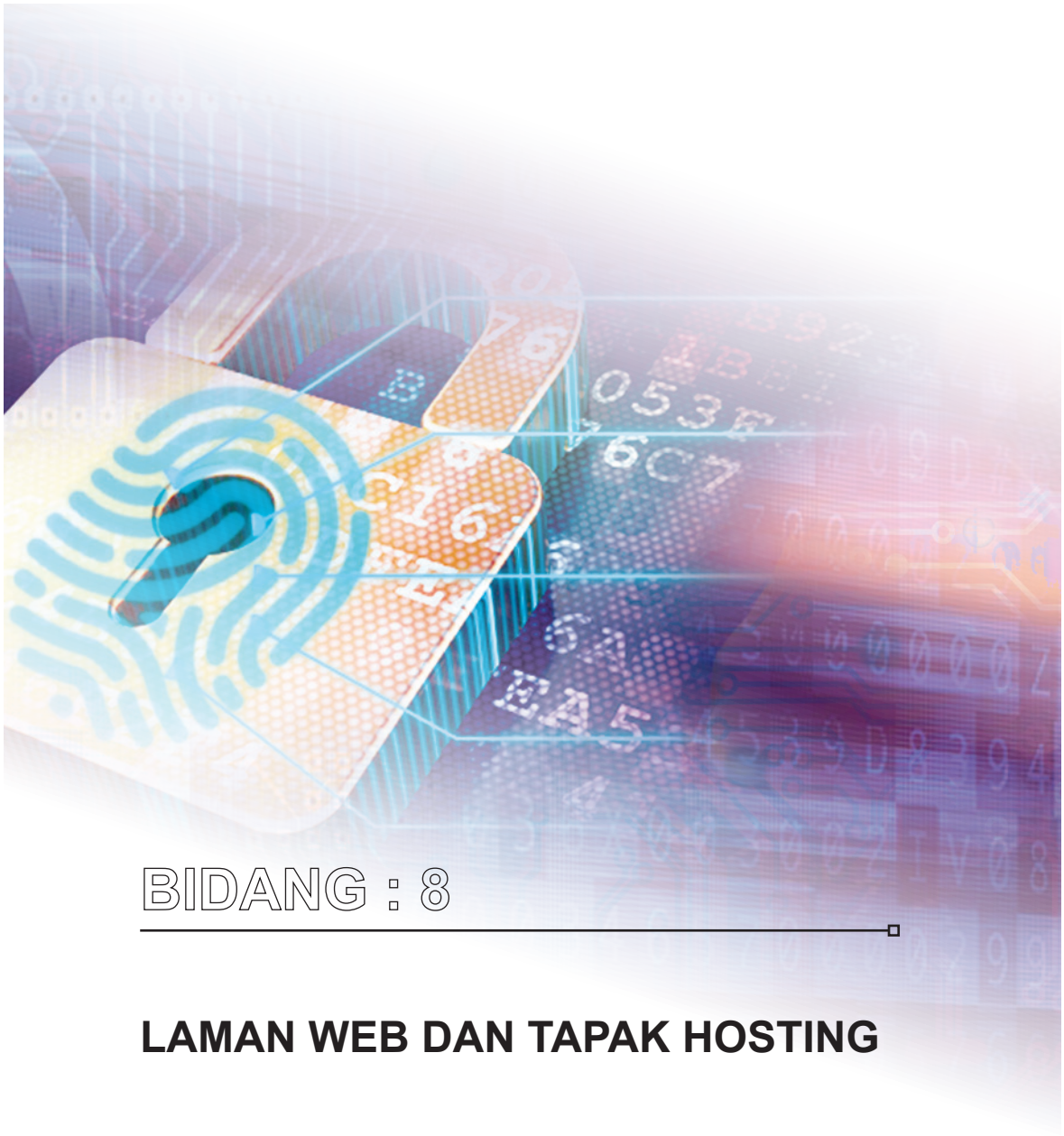
a. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan kehilangan atau pun kerosakan; dan

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

7.6.2 Kerja Jarak Jauh

Perkara yang perlu dipatuhi adalah seperti berikut:

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



BIDANG : 8

LAMAN WEB DAN TAPAK HOSTING

Bidang 8 : **LAMAN WEB DAN TAPAK HOSTING**

8.1 Pembangunan Laman Web dan Tapak Hosting

Objektif :

Untuk menyelaras dan mengawasi pembangunan laman web yang dibangunkan oleh warga UiTM untuk tujuan laman web peribadi bersesuaian seperti mana yang dikehendaki oleh UiTM.

Melibatkan semua pembangunan laman web persendirian yang dibangunkan oleh warga UiTM.

Pemilik laman sesawang mesti mematuhi dasar dan Garis Panduan Pengurusan ICT Universiti, dan bertanggungjawab untuk menjaga integriti sumber dan bahan laman sesawang.

8.1.1 Keperluan Membangun Laman web dan Tapak Hosting

UiTM menggalakkan warga UiTM membangunkan laman web, tetapi hanya laman web rasmi Jabatan/Bahagian/ Fakulti/Kampus Negeri atau seumpamanya sahaja yang boleh dipautkan dalam laman web rasmi UiTM.

Beberapa langkah-langkah perlu dipatuhi oleh pengguna atau pemilik laman web:-

a. Pengguna atau pemilik laman web adalah bertanggungjawab sepenuhnya terhadap semua kandungan. Pihak UiTM tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh pemilik laman web;

b. Pengurusan ICT Universiti berhak menentukan perisian pembangunan laman web bagi tujuan pengoptimumkan penggunaan dan keselamatan;

c. Keselamatan maklumat dan penyiaran adalah di bawah tanggungjawab individu (pemilik laman web) atau PTJ/Kampus Negeri dan perlu mengambil kira aspek keselamatan daripada pencerobohan pihak luar;

d. Pengguna atau pemilik laman web perlu memastikan bahawa laman web peribadi hendaklah berbentuk ilmiah dan bagi tujuan akademik;

e. Laman web yang berunsur politik, perniagaan dan pengiklanan adalah tidak di benarkan sama sekali;

f. Pengiklanan komersial seperti *banner*, *Ads Adsense Google* atau mana-mana yang seumpamanya adalah tidak dibenarkan sama sekali diletakkan di dalam laman web individu;

g. Kandungan laman web tidak boleh mengandungi maklumat yang menyalahi undang-undang / peraturan UiTM, negeri dan negara. Ini termasuk (tetapi tidak terhad kepada) maklumat yang berbentuk politik, keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian;

h. Tidak memberi atau membenarkan dengan sengaja orang perseorangan atau individu lain mengendalikan laman web peribadi di atas identiti pemilik;

i. Pemilik laman web dilarang menggunakan laman web yang dibangunkan sebagai jalan keluar *(proxy)* kepada laman web lain yang berada di luar terutamanya yang menyebabkan kerosakan kepada pihak lain atau UiTM dan

j. Pemilik laman web perlu membuat salinan atau *backup* terhadap laman web mereka sendiri.

8.1.2 Penggunaan Hos Maya (*Virtual Hosting*)

a. Setiap pengguna diberikan maksima 500Mb – 1000Mb ruang storan di server induk dan bergantung kepada keperluan mengikut PTJ;

b. Setiap pengguna/pemilik bertanggungjawab terhadap penggunaan tapak yang dihoskan, khususnya terhadap maklumat yang disebarkan secara elektronik melalui laman web mereka dan mempunyai backup terhadap segala maklumat yang dihoskan;

c. Sebarang masalah yang berkaitan dengan tahap penghantaran dan penerimaan data bagi tapak hos hendaklah dirujuk kepada Jabatan Pengurusan ICT / PTJ/Kampus Negeri untuk tindakan selanjutnya; dan

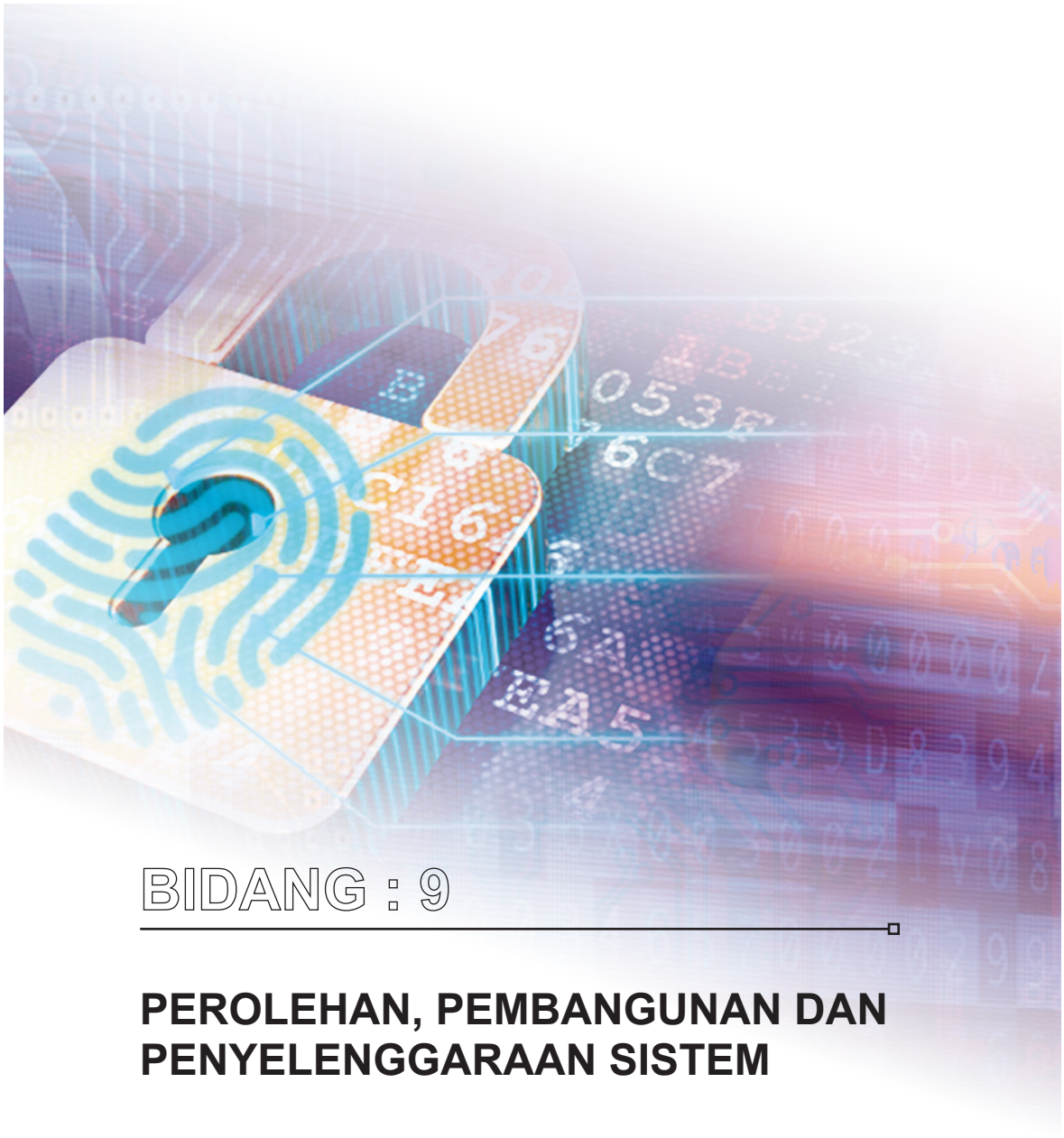
d. Pengguna/pemilik tapak tidak dibenarkan merosakkan sistem komputer atau data dengan apa jua cara seperti pengedaran virus komputer melalui tapak yang dihoskan.

8.1.3 Pelanggaran

a. Jabatan Pengurusan ICT tidak bertanggungjawab ke atas sebarang kerosakan atau kehilangan maklumat pada *server* sehingga menyebabkan berlakunya kegagalan capaian maklumat.

b. UiTM berhak menamatkan mana-mana laman web peribadi yang melanggar syarat-syarat yang dinyatakan tanpa sebarang notis.

c. Jika didapati bahawa sumber maklumat UiTM telah disalahgunakan atau tidak mengikut peraturan yang ditetapkan, Jabatan Pengurusan ICT boleh menghadkan atau membatalkan akses kepada tapak hos tersebut dan seterusnya menamatkan perkhidmatannya.



BIDANG : 9

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Bidang 9 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

9.1 Keselamatan Dalam Membangunkan dan Menyelenggara Sistem Aplikasi

Objektif :

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

9.1.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

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

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

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

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

9.1.2 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

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

9.2 Kawalan Kriptografi

Objektif :

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

9.2.1 Enkripsi

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

9.2.2 Tandatangan Digital

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

9.2.3 Pengurusan Infrastruktur Kunci Awam (*Public Key Infrastructure* (PKI)

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

9.3 Keselamatan Fail Sistem

Objektif :

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

9.3.1 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

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

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

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

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

9.4 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif :

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

9.4.1 Prosedur Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

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

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

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

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

e. Menghalang sebarang peluang untuk membocorkan maklumat.

9.4.2 Pembangunan aplikasi Secara *Inhouse/Outsource/Joint Venture*

Pembangunan aplikasi secara *inhouse/outsource/joint venture* perlu diselia dan dipantau sentiasa oleh pemilik sistem.

a. Aspek teknikal perlu dikawalselia oleh Pengurusan ICT.

b. Klausa mengenai pemindahan teknologi (*Transfer of Technology*) dan penyerahan serta pemilikan *source code* dari pembekal kepada Pengurusan ICT/PTJ hendaklah dinyatakan dalam dokumen kontrak. Ini bagi memastikan kerja-kerja penyelenggaraan dapat dikawalselia oleh Pengurusan ICT/ PTJ.

c. Pihak ketiga perlulah menyediakan dokumentasi manual pengguna dan dokumentasi sistem yang lengkap dan terkini kepada Pengurusan ICT/PTJ.

Proses perolehan pembangunan aplikasi secara *outsource* perlu mengikut Garis Panduan Pengurusan ICT Universiti dan peraturan semasa yang telah ditetapkan.

9.5 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif :

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

9.5.1 Kawalan dari Ancaman Teknikal

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

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

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

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

9.6 Keselamatan Perisian Sistem Aplikasi

Pentadbir Sistem ICT adalah bertanggungjawab memastikan kawalan keselamatan dilaksana bagi mengelak berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat.

Pengurusan ICT bertanggungjawab menyediakan kawalan dan kemudahan seperti berikut:

a. Sistem keselamatan berpusat dengan kawalan capaian penggunaan satu ID dan kata laluan untuk semua aplikasi berpusat;

b. Profil capaian yang menghadkan tahap capaian maklumat serta fungsi berdasarkan peranan pengguna;

c. Kawalan peringkat sistem aplikasi dengan mengadakan sistem log yang menentukan akauntabiliti kepada semua pengguna; dan

d. Penetapan pemilik maklumat adalah merujuk kepada pemilik sistem.

9.7 Keselamatan Pangkalan Data

Kawalan perlu dilaksanakan untuk menghalang capaian kepada pangkalan data dari sebarang pengubahsuaian atau pemusnahan data secara tidak sah.

Pentadbir Sistem ICT adalah bertanggungjawab ke atas integriti maklumat yang disimpan dalam pangkalan data kekal dan terjamin serta mengikut Garis Panduan Pengurusan ICT Universiti dan peraturan semasa yang telah ditetapkan.

Integriti maklumat yang disimpan di dalam pangkalan data boleh dikekalkan melalui:

a. Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data;

b. Sistem pengurusan pangkalan data yang memastikan integriti dalam pengemaskinian dan capaian maklumat. Kawalan perlu dilaksanakan untuk pangkalan data yang dikongsi bersama; dan

c. Mekanisme kawalan capaian kepada sumber maklumat fizikal dan pelaksanaan tugas-tugas rutin pangkalan data seperti :

    i. semakan *database consistency*;

    ii. semakan penggunaan ruang storan ;

    iii. pemantauan aktiviti pangkalan data;

    iv. pemantauan aktiviti server dan pengguna ;

    v. melaksanakan *backup* dan *restore*; dan

    vi. performance tuning.

9.8 Perubahan Versi

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

9.9 Penyimpanan Kod Sumber (*Source Code*)

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

a. Mewujudkan prosedur penyelenggaraan versi terkini;

b. Mendokumenkan prosedur *backup* kod sumber bagi penyelenggaraan versi terkini; dan

c. Menyimpan *backup* kod sumber di lokasi yang berasingan.

Antara langkah-langkah yang perlu diambil bagi memastikan integriti sistem aplikasi tidak terdedah kepada sebarang pencerobohan keselamatan:

a. Melaksanakan *patches* bagi mengatasi kelemahan sistem;

b. Dapatkan *patches* yang terkini daripada agensi keselamatan berdaftar seperti MyCERT (*Malaysian Computer Emergency Response Team*) di alamat web http://www.mycert.org.my/, Microsoft atau syarikat perisian yang berkaitan;

c. Melakukan peningkatan (*upgrades*) perisian dan firmware; dan

d. Wujudkan prosedur pengemaskinian sistem pengoperasian daripada serangan dan ancaman.

9.10 Pengujian Aplikasi

Pentadbir Sistem ICT adalah bertanggungjawab menguji atucara, modul, sistem aplikasi dan integrasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan. Bagi menghalang maklumat daripada didedah atau diproses secara tidak sepatutnya, persekitaran yang berbeza untuk pembangunan sistem dan pengoperasian sistem perlu diwujudkan.

Sekiranya persekitaran berasingan untuk pembangunan sistem tidak dapat dilaksanakan, langkah-langkah berikut hendaklah dilakukan:

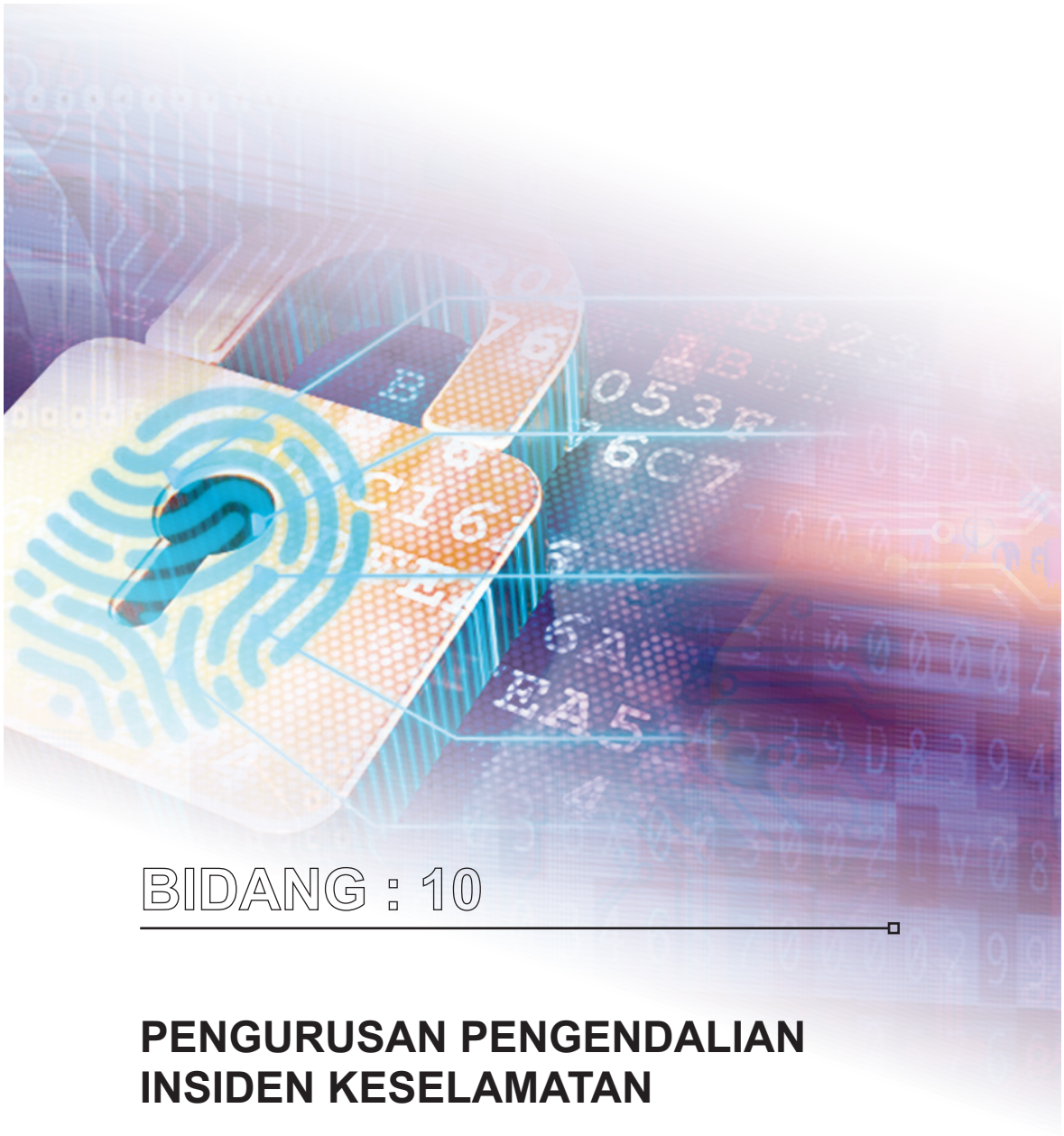
a. Menggunakan data ujian (*dummy*) atau data lapuk (*historical)*;

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

c. Menghadkan capaian kepada staf yang terlibat sahaja;

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

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



BIDANG : 10

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Bidang 10 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

10.1 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

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

10.1.1 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan UiTMCERT 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;

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

f. Prosedur pelaporan insiden keselamatan ICT berdasarkan:

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

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

10.2 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif :

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

10.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada UiTM. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan.

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

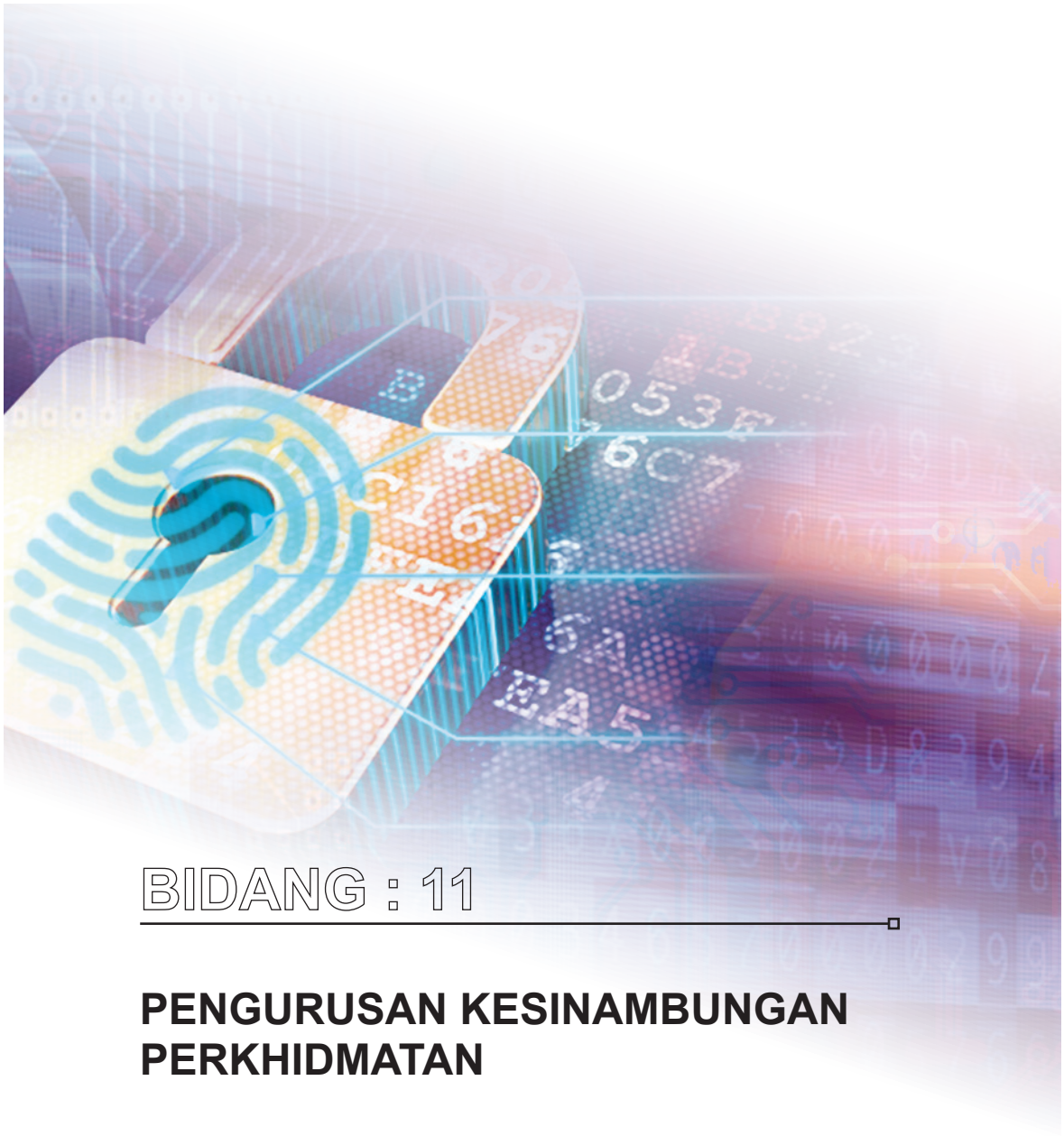
a. Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;

b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

d. Menyediakan tindakan pemulihan segera; dan

e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.



BIDANG : 11

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Bidang 11 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

11.1 Dasar Kesinambungan Perkhidmatan

Objektif :

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

11.1.1 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan *(Business Continuity Management*, BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi.

Walaubagaimanapun, Pelan Pemulihan Bencana (*Disaster Recovery Planning* (DRP)) merupakan pelan kesinambungan perkhidmatan bagi ICT yang yang dibangunkan pihak Pengurusan ICT universiti bagi memastikan perkhidmatan ICT dapat diteruskan.

Pelan ini mestilah diluluskan oleh Unit Pengurusan Risiko UiTM dan perkara-perkara berikut perlu diberi perhatian:

a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

b. Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap operasi ICT UiTM bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;

c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;

e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

f. Membuat penduaan; dan

g. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

Pelan DRP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

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

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

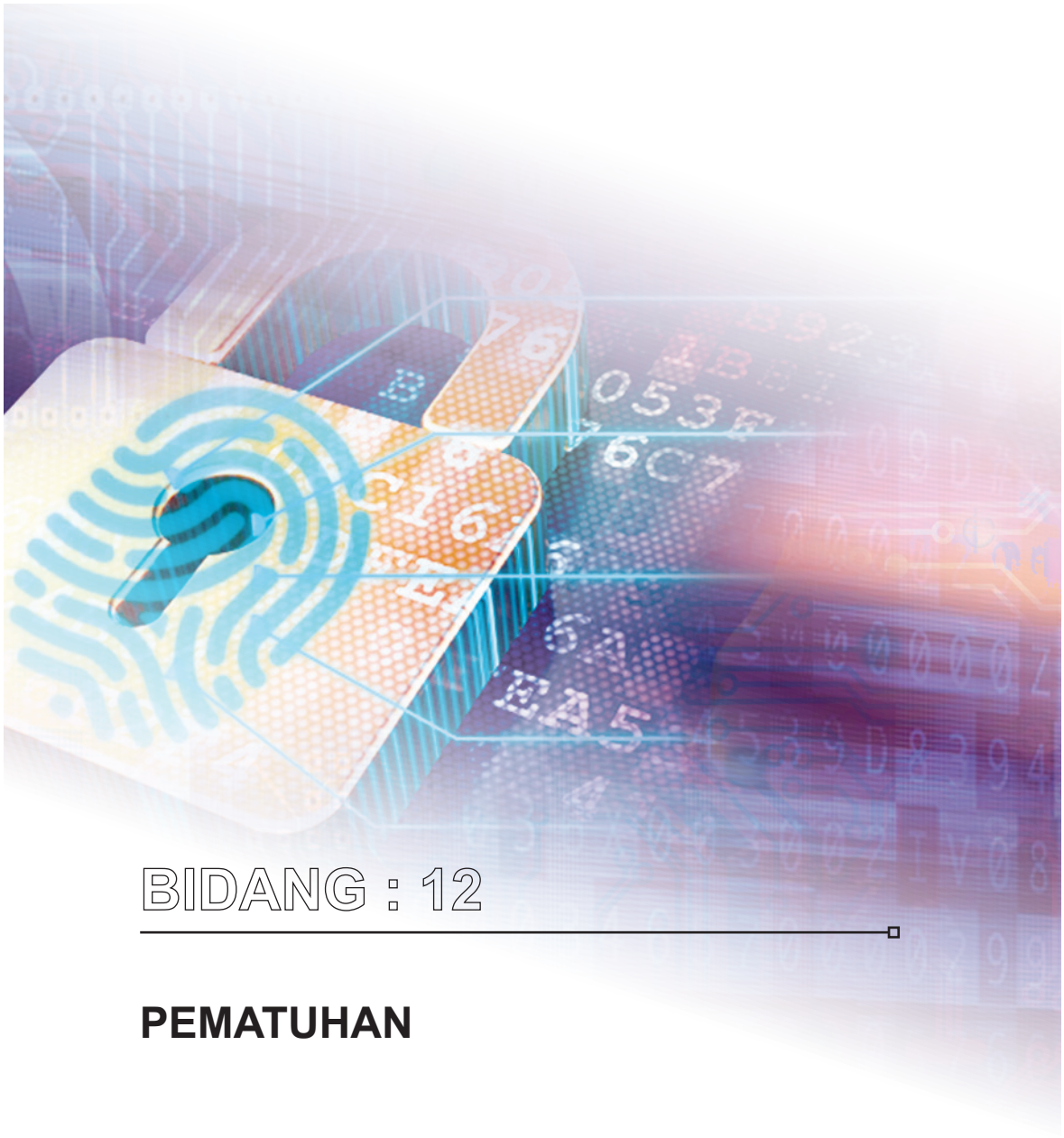
d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

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

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

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

UiTM hendaklah memastikan salinan pelan DRP sentiasa dikemaskini dan dilindungi seperti di lokasi utama.



BIDANG : 12

PEMATUHAN

Bidang 12 : **PEMATUHAN**

12.1 Pematuhan dan Keperluan Perundangan

Objektif :

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKICT UiTM.

12.1.1 Pematuhan Dasar

Setiap pengguna di UiTM hendaklah membaca, memahami dan mematuhi DKICT UiTM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

Semua aset ICT di UiTM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah atau pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT UiTM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber UiTM.

12.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

12.1.3 Pematuhan Keperluan Audit

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

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

12.1.4 Pelanggaran Dasar

Pelanggaran DKICT UiTM dan dasar di bawahnya boleh dikenakan tindakan tatatertib.

BIDANG : 13

PEMAKAIAN DASAR, PEKELILING DAN GARIS PANDUAN ICT SEMASA PERINGKAT KEBANGSAAN

Bidang 13 : PEMAKAIAN DASAR, PEKELILING DAN GARIS PANDUAN ICT SEMASA PERINGKAT KEBANGSAAN

13.1 Pemakaian Dasar, Pekeliling dan Garis Panduan ICT

DKICT ini tidak terhad kepada kandungan dokumen ini, malah ianya hendaklah dibaca bersama dengan dasar, pekeliling dan garis panduan ICT peringkat kebangsaan yang dikuatkuasakan seperti berikut:

a. Undang-undang Siber (Cyber Law) yang diperkenalkan oleh kerajaan di bawah program MSC Bill of Guarantees yang terdiri daripada akta berikut:

   ii. Tandatangan Digital 1997;

   iii. Hakcipta (amendment) 1997;

   iv. Jenayah Komputer 1997;

   v. Tele-medicine 1997;

   vi. Komunikasi dan Multimedia 1998; dan (vi) Suruhanjaya Komunikasi dan Multimedia Malaysia 1998.

b. Akta:

   i. Akta Aktiviti Kerajaan Elektronik (EGAA) 2007 [Akta 680];

   ii. Akta Aktiviti Kerajaan Elektronik (EGAA) 2000; dan (iii) Akta Perlindungan Data Peribadi 2010.

c. Pekeliling Am yang terdiri daripada berikut:

   i. Pekeliling Am Bil. 6 Tahun 1999: Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan dalam Bidang Teknologi Maklumat yang dikeluarkan oleh MAMPU;

   ii. Pekeliling Am Bil. 2 Tahun 1999: Penubuhan Jawatankuasa IT dan Internet Kerajaan (JITIK) yang dikeluarkan oleh MAMPU;

   iii. Pekeliling Am Bil. 3 Tahun 2000: Dasar Keselamatan ICT Kerajaan yang dikeluarkan oleh MAMPU;

iv. Pekeliling Am Bil.1 Tahun 2000: Garis Panduan Malaysian *Civil Service Link (MCSL)* dan Laman Web Kerajaan yang dikeluarkan oleh MAMPU;

v. Pekeliling Am Bil.1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan ICT yang dikeluarkan oleh MAMPU;

vi. Pekeliling Am Bil. 2 Tahun 2002: Penggunaan dan Pemakaian Data Dictionary Sektor Awam (DDSA) Sebagai Standard di Agensi-agensi Kerajaan;

vii. Pekeliling Am Bil. 1 Tahun 2006: Pengurusan Laman Web/ Portal Sektor Awam; dan

viii. Pekeliling Am Bil. 2 Tahun 2006: Pengukuhan Tadbir Urus Jawatankuasa IT dan Internet Kerajaan.

d. Surat Arahan KP (Ketua Pengarah MAMPU);

e. Surat Arahan KSN (Ketua Setiausaha Negara);

f. Surat Pekeliling Am;

i. Surat Pekeliling Am Bil. 1 Tahun 2009: Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan yang dikeluarkan oleh MAMPU;

ii. Surat Pekeliling Am Bilangan 3 Tahun 2009: Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam;

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

iv. Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

v. Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) yang dikeluarkan oleh MAMPU.

vi. Akta, pekeliling, arahan, garis panduan dan surat pekeliling baharu serta pindaan-pindaan kepada Akta, pekeliling, arahan, garis panduan dan surat pekeliling sedia ada yang dikeluarkan oleh kerajaan dari semasa ke semasa.

GLOSARI

Pernyataan	Definisi
UiTM	Universiti Teknologi MARA
CIO	Ketua Pegawai Maklumat (Chief Information Officer) Ketua Pegawai maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
JPPIT	Jawatankuasa Pembangunan Projek IT UiTM
PTJ	Pusat Tanggungjawab bermaksud jabatan, fakulti, pejabat, pusat, kampus kota, kampus negeri di UiTM
Pengurus ICT	Ketua-ketua jabatan
Pentadbir ICT	Staf PTM/PTMK yang bertanggungjawab.
Pentadbir Sistem	Pegawai yang bertanggungjawab untuk membangun, mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan kemudahan ICT.
Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada sepenuh masa atau separuh masa) di UiTM dan statusnya masih aktif.
Pengguna	Staf pelajar UiTM dan pihak ketiga yang menggunakan perkhidmatan ICT di UiTM
PTM	Pegawai Teknologi Maklumat
PTMK	Pegawai Teknologi Maklumat Kanan
PPTM	Penolong Pegawai Teknologi Maklumat
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada UiTM. Pembekal, pakar runding dan lain-lain yang terlibat secara langsung dengan pengurusan Universiti

Akaun Pengguna	Akaun Pengguna merupakan satu kaedah bagi membenarkan seseorang pengguna untuk membuat capaian terhadap sesuatu sistem. Kebiasaanya akaun pengguna melibatkan penggunaan kata nama dan kata laluan.
MAMPU	Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri
LAN	*Local Area Network* Rangkaian komputer yang merangkumi rangkaian kawasan setempat. LAN dalam skop UiTM adalah rangkaian UiTM di Shah Alam, kampus negeri dan kampus kota UiTM.
WAN	*Wide Area Network* Rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer yang berada pada lokasi yang berbeza (negeri, negara dan benua). WAN dalam skop UiTM adalah sambungan kepada rangkaian Internet.
MAN	*Metropolitan Area Network* Rangkaian computer yang meliputi suatu kawasan geografi yang agak luas berbanding dengan rangkaian yang diliputi oleh LAN. MAN dalam skop UiTM adalah rangkaian yang merangkumi UiTM Kampus Negeri/ UiTM Kampus PFI, dan UiTM kampus kota/satelit
PFI	*Private Funding Initiative* Konsep kampus yang dibangunkan menerusi pembiayaan pihak swasta. Pihak swasta yang di kenalpasti yang akan membiayai kos pembiayaan dan penyelenggaraan buat kampus di negeri-negeri yang telah dikenalpasti.

Kod Sumber Sistem Aplikasi	Merujuk kepada sebarang pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia dan terdapat dalam beberapa fail computer tetapi kod sumber yang sama boleh dicetak di dalam buku atau dirakam dalam pita.
Kemudahan ICT	Merujuk kepada perkakasan, peralatan dan perkhidmatan yang berkaitan teknologi maklumat dan telkomunikasi yang disediakan oleh UiTM bagi tujuan pengurusan, pentadbiran, penyelidikan, pengajaran dan pembelajaran serta operasi pengguna.
Server	Bermaksud computer yang mempunyai keupayaan tinggi yang member perkhidmatan berpusat.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Negara Malaysia, hendaklah diperingkatkan Rahsia Besar.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan atau mertabat negara Malaysia atau member keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan Rahsia.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Negara tetapi memudaratkan kepentingan atau mertabat negara Malaysia atau kegiatan kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan Sulit.

Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan hendaklah diperingkatkan Terhad.
Insiden Keselamatan	Musibah *(adverse event)* yang berlaku ke atas system maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (soft copy), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera padatm cakera mudah alih, pita, cakera keras dan pemacu pena.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab UiTM
Akaun Pengguna	Akaun e-mel, e-community dan rangkaian
Kawasan Terperingkat	Kawasan-kawasan premis atau sebahagian dari premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Peralatan Perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti firewall, router, proxy dan antivirus.
Enkripsi	Bermaksud menjadikan teks biasa (plain text) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks cipher. Bagi mendapatkan semula teks biasa tersebut, penyahsulitan digunakan.

Kriptografi	Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
Internet	Internet adalah sistem rangkaian komunikasi global. Ia merangkumi infrastruktur perkakasan dan perisian yang menyediakan sambungan rangkaian global di antara komputer.Internet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di seluruh dunia secara atas talian.
Intranet	Merujuk kepada jaringan rangkaian dalaman yang menghubungkan komputer di dalam sesebuah organisasi dan hanya boleh dicapai oleh staf atau mana-mana pihak yang dibenarkan. Intranet dalam skop UiTM adalah servis rangkaian yang membolehkan pengguna mengakses sumber maklumat di dalam kampus UiTM secara atas talian.
VPN	Virtual Private Network - Rangkaian Persendirian Maya Servis rangkaian yang menggunakan infrastruktur telekomunikasi awam seperti Internet bagi membolehkan pengguna yang berada di luar kampus mendapat capaian Metro-E dan menggunakan rangkaian tersebut dalam keadaan selamat.
Public IP	Alamat IP yang dikhaskan untuk kegunaan rangkaian luar seperti WAN (internet).
Private IP	Alamat IP yang dikhaskan untuk rangkaian dalaman seperti LAN dan MAN dan tidak di sebarkan ke internet.
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.

Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di anatara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi 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).*
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan IT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

Hub	Hab *(hub)* merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer.* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
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 computer yang memantau rangkaian dan/atau aktivti 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.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi 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
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui internet.
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 pengasingan rangkaian dapat dilakukan. 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 peribadi dan atas sebab tertentu.
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 Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
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.
Kesinambungan Perkhidmatan	Merujuk kepada perkhidmatan dan pelaksanaan fungsi kritikal serta proses-proses utama yang berterusan walaupun berlaku gangguan dan fungsi-fungsi normal segera dibaik pulih dalam tempoh masa yang ditetapkan.
Penilaian Risiko	Penilaian risiko atau risk assessment merujuk kepada penilaian ke atas kebarangkalian menghadapi gangguan dan kesan dari kerosakan atau kehilangan aset.

Pasukan PKP	Merupakan pasukan yang dipertanggungjawabkan ke atas projek Pengurusan Kesinambungan Perkhidmatan di agensi. Ahli Pasukan PKP terdiri daripada wakil Bahagian, Unit atau Cawangan di agensi dan diketuai oleh Koordinator PKP.
Simulasi	Simulasi adalah proses menguji pelan pelaksanaan PKP agensi untuk mengenal pasti isu dan kekurangan dalam dokumentasi.
Pelan Kesinambungan Perkhidmatan	Pelan Kesinambungan Perkhidmatan merujuk kepada pelan atau perancangan pengurusan kesinambungan perkhidmatan. Perancangan ini yang meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan kepada system penyampaian perkhidmatan perlu didokumenkan, diuji dan dikaji semula secara berkala dan dilaksanakan apabila berlaku gangguan. Di samping itu, tindakan dilaksanakan untuk segera membaik pulih pelaksanaan fungsi-fungsi normal university dalam tempoh yang ditetapkan.
Pusat Pemulihan Bencana	Pusat pemulihan bencana atau disaster recovery centre merupakan lokasi alternatif bagi lokasi asal untuk membolehkan agensi meneruskan operasi ICT yang menyokong fungsi kritikal agensi apabila berlaku gangguan atau bencana.
Pelan Pemulihan Bencana	Pelan Pemulihan Bencana atau Disaster Recovery Plan merujuk kepada dokumen pelan yang menetapkan sumber, tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan dalam perkhidmatan agensi. Pelan ini direka bentuk untuk membantu agensimengembalikan semula proses perkhidmatan dalam tempoh ditetapkan untukpemulihan bencana.

Pelan Simulasi	Dokumen perancangan yang digunakan bagi proses simulasi atau menguji tindakan-tindakan yang perlu dilaksanakan oleh Pasukan PKP apabila pelan (kesinambungan perkhidmatan/ pemulihan bencana/ pengurusan krisis) diaktifkan. Pelaksanaannya mungkin melibatkan Pasukan PKP atau semua warga organisasi dan dilaksanakan dalam keadaan atau situasi yang seakan-akan gangguan atau bencana sebenar.

LAMPIRAN

LAMPIRAN A

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT
UNIVERSITI TEKNOLOGI MARA

Nama : .....

No Kad Pengenalan : .....

Jawatan : .....

PTJ/Jabatan/Organisasi : .....

No Telefon : .....

Adalah dengan ini sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT UiTM; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....
(Tandatangan)
Tarikh: .....

Pengesahan Pegawai Keselamatan ICT,

.....
_____
(Nama Pegawai Keselamatan ICT)