DASAR KESELAMATAN ICT (DKICT) UNIMAS

UNIMAS ICT SECURITY POLICY

VERSI : 7.1

TARIKH : 4 Julai 2024

REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/ PINDAAN	BAB/ MUKA SURAT	KETERANGAN PINDAAN
14 November 2012	1.0	-	Baharu
5 Mei 2013	2.0	-	Rujuk Borang Cadangan Pindaan Dokumen PKTMK Bil 1/Tahun 2013
10 September 2013	3.0	-	Rujuk Borang Cadangan Pindaan Dokumen PKTMK Bil 52/Tahun 2013
10 September 2013	3.0	-	Rujuk Borang Cadangan Pindaan Dokumen PKTMK Bil 53/Tahun 2013
14 Julai 2015	4.0	-	Rujuk Borang Cadangan Pindaan Dokumen PKTMK Bil 23/2015
9 September 2015	4.1	-	Rujuk Borang Cadangan Pindaan Dokumen PKTMK Bil 5/2015
8 Februari 2017	5.0	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 1/2017
30 Ogos 2018	6.0	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 8/2018
22 Februari 2019	6.1	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 11/2018
11 September 2019	6.2	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 13/2018
13 Oktober 2020	6.3	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 2/2020
30 November 2021	6.4	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 2/2021
14 September 2022	6.5	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 3/2022
27 Januari 2023	6.5	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 1/2023
13 Sep 2023	7.0	-	Rujuk Borang Cadangan Pindaan Dokumen CITDS Bil 7/2023
4 Julai 2024	7.1	-	Rujuk Borang Cadangan Pindaan Dokumen TAHODC Bil 4/2024

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) UNIMAS mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT UNIMAS.

OBJEKTIF

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

Manakala, objektif utama Keselamatan ICT UNIMAS ialah seperti berikut:

(a) Memastikan kelancaran operasi UNIMAS 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 kerajaan.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah,
2. Menjamin setiap maklumat adalah tepat dan sempurna,
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

DKICT UNIMAS merangkumi perlindungan ke atas semua bentuk maklumat bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

1. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran,
2. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.
3. Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal, serta dijamin kesahihannya; dan

4. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT UNIMAS dan perlu dipatuhi adalah seperti berikut:

1. 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.

2. 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.

3. Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

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

4. Pengasingan

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

5. Pengauditan

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

6. Pematuhan

DKICT UNIMAS hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk kelalaian yang boleh membawa ancaman kepada keselamatan negara.

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT (DKICT)

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

010101 Perlaksanaan Dasar

Perkara	Tanggungjawab
Pelaksanaan dasar ini akan dijalankan oleh Chief Digital Officer UNIMAS selaku Pengerusi Jawatankuasa Pemandu ICT UNIMAS. Jawatankuasa ini terdiri daripada semua TNC, Bendahari, Pendaftar, Pengarah TAHODC, Pengarah PeTARY, Pengarah RIEC, Pengarah PPGM, Pengarah PPPU, Pengarah PPS, semua Dekan Fakulti dan Pegawai Keselamatan ICT (ICTSO).	Chief Digital Officer, CDO

010102 Penyebaran Dasar

Perkara	Tanggungjawab
Dasar ini perlu disebarkan kepada semua pengguna UNIMAS dan pihak ketiga.	ICTSO

010103 Penyelenggaraan Dasar

Perkara	Tanggungjawab
DKICT UNIMAS 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 UNIMAS: (a) Kenal pasti dan tentukan perubahan yang diperlukan, (b) Pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT UNIMAS, (c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh Jawatankuasa Pemandu ICT UNIMAS; dan (d) Mengkaji semula dasar sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	ICTSO
010104 Pengecualian Dasar	
Perkara	**Tanggungjawab**
DKICT UNIMAS adalah terpakai kepada semua pengguna UNIMAS dan pihak ketiga tanpa ada sebarang pengecualian.	Semua
BIDANG 02 ORGANISASI KESELAMATAN	
0201 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan	

teratur dalam mencapai objektif DKICT UNIMAS.

020101 Ketua Pegawai Digital (CDO)

Perkara	Tanggungjawab
Ketua Pegawai Digital (CDO) bagi UNIMAS adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami dan mematuhi DKICT UNIMAS, (b) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan (c) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT UNIMAS.	CDO

020102 Ketua Pegawai Teknologi Maklumat (CTO)

Perkara	Tanggungjawab
Ketua Pegawai Teknologi Maklumat (CTO) bagi UNIMAS ialah Pengarah TAHODC. Peranan dan tanggungjawab CTO adalah seperti berikut: (a) Menyelaras keseluruhan program-program keselamatan ICT UNIMAS, (b) Menguatkuasakan pelaksanaan DKICT UNIMAS, (c) Mengesahkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT UNIMAS, (d) Melaporkan insiden keselamatan ICT kepada CDO; dan (e) Bertanggungjawab ke atas perkara-perkara yang berkaitan	CTO

dengan keselamatan ICT UNIMAS.	

020103 Pegawai Keselamatan ICT (ICTSO)

Perkara	Tanggungjawab
Pegawai Keselamatan ICT (ICTSO) bagi UNIMAS ialah Pegawai Teknologi Maklumat (PTM) TAHODC Gred 48 ke atas. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus program-program keselamatan ICT UNIMAS, (b) Memberi penerangan dan pendedahan berkenaan DKICT UNIMAS kepada semua pengguna, (c) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT UNIMAS, (d) Menjalankan pengurusan risiko, (e) Menjalankan audit, mengkaji semula, merumus tindak balas berdasarkan hasil penemuan keselamatan ICT dan menyediakan laporan mengenainya kepada Pengurusan UNIMAS, (f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian, (g) Menerima dan melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT UNIMAS (UNIMAS-CSIRT), dan memaklumkannya kepada CTO, (h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera, (i) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan (j) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT.	ICTSO

020104 Pengurus ICT

Perkara	Tanggungjawab
Pengurus ICT bagi UNIMAS ialah Pegawai Teknologi Maklumat (PTM). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan UNIMAS, (b) Menentukan kawalan akses pengguna terhadap aset ICT UNIMAS, (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT UNIMAS.	Pengurus ICT

020105 Pentadbir Sistem ICT

Perkara	Tanggungjawab
Pentadbir Sistem ICT bagi UNIMAS ialah Pegawai Teknologi Maklumat, Penolong Pegawai Teknologi Maklumat, Penolong Jurutera atau Juruteknik Komputer. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai staf yang berhenti, bertukar, bercuti panjang, berkursus panjang atau berlaku perubahan dalam bidang tugas,	Pentadbir Sistem ICT

(b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sistem maklumat, (c) Memantau aktiviti capaian sistem aplikasi pengguna, (d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta, (e) Menganalisis dan menyimpan rekod jejak audit, (f) Menjalankan semakan semula capaian secara berkala; dan (g) Bertanggungjawab memantau setiap aset ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	

020106 Pengguna

Perkara	**Tanggungjawab**
Pengguna bagi UNIMAS terdiri daripada semua staf UNIMAS yang merangkumi staf tetap/kontrak/sambilan/dipinjamkan/sementara dan pelajar. Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi DKICT UNIMAS, (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya, (c) Melaksanakan prinsip-prinsip DKICT UNIMAS dan menjaga kerahsiaan maklumat UNIMAS, (d) Melaporkan sebarang aktiviti yang mencurigakan atau mengancam keselamatan ICT kepada ICTSO dengan segera; dan (e) Menghadiri program-program kesedaran mengenai keselamatan ICT.	Pengguna

020107 Pasukan Tindak Balas Insiden Keselamatan ICT UNIMAS (UNIMAS-CSIRT)

Perkara	Tanggungjawab
UNIMAS-CSIRT dipengerusikan oleh ICTSO. Jawatankuasa ini terdiri daripada pegawai yang terlibat dalam pembangunan sistem aplikasi, rangkaian, Pusat Data, sokongan teknikal dan wakil skim F (Gred 29 ke atas) di PTj. Peranan dan tanggungjawab UNIMAS-CSIRT adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden, (b) Merekod dan menjalankan siasatan awal insiden yang diterima, (c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih, (d) Menghubungi dan melapor insiden yang berlaku kepada NACSA (jika perlu), (e) Menasihati pihak berkaitan mengambil tindakan pemulihan dan pengukuhan, (f) Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada Pengguna; dan (g) Menjalankan penilaian untuk memastikan keselamatan ICT pada tahap yang baik dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT.	ICTSO

020108 Jawatankuasa Pemandu ICT UNIMAS

Perkara	Tanggungjawab
Jawatankuasa Pemandu ICT UNIMAS adalah jawatankuasa yang bertanggungjawab sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi ICT UNIMAS. Peranan dan tanggungjawab Jawatankuasa Pemandu ICT UNIMAS adalah seperti berikut: a) Memperakukan dokumen dasar ICT UNIMAS; dan b) Memastikan DKICT UNIMAS selaras dengan dasar-dasar ICT kerajaan semasa,	Chief Digital Officer

0202 Pihak Ketiga

Objektif:
Menjamin keselamatan semua aset ICT yang diguna oleh pihak ketiga (pembekal, pakar runding, pihak berkepentingan, agensi luar dan lain-lain).

020201 Keperluan Keselamatan Melibatkan Pihak Ketiga

Perkara	Tanggungjawab
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal dengan rapi. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi DKICT UNIMAS, (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan	Naib Canselor, CDO, CTO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pihak Ketiga

pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran ke atas capaian maklumat, (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga, (d) Akses kepada aset ICT UNIMAS perlu berlandaskan kepada perjanjian kontrak (e) Pembekal bertanggungjawab untuk membaikpulih sebarang kerosakan kesan daripada kerja-kerja pemasangan atau penyelenggaraan secara sengaja atau sebaliknya. Pihak ketiga bertanggungjawab menanggung segala implikasi kos yang terlibat. (f) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT (DKICT) UNIMAS, dan/atau ii. *Non-Disclosure Agreement* (NDA); dan (g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT UNIMAS seperti di Lampiran 1.	
BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT UNIMAS.	
030101 Aset Alih ICT	

Perkara	Tanggungjawab
Ini bertujuan memastikan semua aset alih 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 alih ICT dikenalpasti, didaftarkan dan maklumatnya direkod dan sentiasa dikemaskini dalam KEW.PA-2 bagi borang daftar harta modal (Rujuk Lampiran 5) dan KEW.PA-3 bagi inventori (Rujuk Lampiran 6), (b) Memastikan semua aset alih ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja, (c) Memastikan Pegawai Aset PTj mengurus dan mengawal penempatan aset alih ICT yang ditempatkan di PTj masing-masing, (d) Peraturan bagi pengendalian aset alih ICT hendaklah dikenal pasti, didokumen dan dilaksanakan, (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset alih ICT dibawah kawalannya serta mematuhi UNIMAS ICT Usage Policy, UNIMAS ICT Governance Policy; dan (f) Mematuhi Tatacara Pengurusan Aset Alih UNIMAS.	Pentadbir Sistem dan Pengguna (tidak termasuk Pelajar)
0302 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset alih ICT diberikan tahap perlindungan yang bersesuaian.	

030201 Pengelasan Maklumat

Perkara	Tanggungjawab
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh staf yang diberi kuasa mengikut dokumen Arahan Keselamatan Kerajaan Malaysia. 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.	Pengguna (tidak termasuk Pelajar)

030202 Pengendalian Maklumat

Perkara	Tanggungjawab
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan, (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa, (c) Menentukan maklumat sedia untuk digunakan, (d) Menjaga kerahsiaan kata laluan, (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan,	Semua

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan maklumat daripada diketahui umum.	

BIDANG 04 KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk staf UNIMAS dan pihak ketiga memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pihak berkenaan hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

040101 Sebelum Pengesahan dalam Perkhidmatan

Perkara	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan	Pengguna (tidak termasuk Pelajar)

040102 Dalam Perkhidmatan

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan staf UNIMAS serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT mestilah berdasarkan perundangan dan peraturan yang ditetapkan oleh UNIMAS, (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT UNIMAS secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa, (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas staf UNIMAS serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh UNIMAS; 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. Merujuk kepada Pusat Kepimpinan UNIMAS, untuk sebarang keperluan kursus dan latihan teknikal yang berkaitan.	Semua (tidak termasuk Pelajar)

040103 Bertukar Atau Tamat Perkhidmatan

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada UNIMAS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan	Semua (tidak termasuk Pelajar)

(b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan ICT mengikut peraturan yang ditetapkan oleh UNIMAS dan/atau terma perkhidmatan.	

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

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

050101 Kawalan Kawasan

Perkara	Tanggungjawab
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko, (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan ICT, (c) Memasang alat penggera atau kamera/CCTV, (d) Menghadkan jalan keluar masuk,	Pengarah Bahagian Keselamatan, CDO, CTO dan ICTSO

(e) Mengadakan kawalan di kaunter perkhidmatan, (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat, (g) Menyediakan *staging room* untuk kerja-kerja penerimaan, pemasangan dan konfigurasi aset ICT. (h) Mewujudkan perkhidmatan kawalan keselamatan di pintu masuk, (i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan staf yang diberi kebenaran sahaja boleh melalui pintu masuk ini, (j) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan, (k) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	

050102 Kawalan Masuk Fizikal

Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap staf/pelajar UNIMAS hendaklah membawa pengenalan identiti staf/pelajar sepanjang berada di UNIMAS, (b) Semua kad staf hendaklah dikembalikan kepada UNIMAS apabila pengguna tamat perkhidmatan, (c) Pelawat hendaklah mendapatkan pas pelawat di pintu kawalan keselamatan utama UNIMAS, (d) Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan	Semua

(e) Kehilangan pas pelawat/kad staf/kad pelajar mestilah dilaporkan dengan segera.	

050103 Kawasan Larangan

Perkara	Tanggungjawab
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pengguna dan pihak ketiga yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di UNIMAS adalah bilik Naib Canselor, Timbalan-timbalan Naib Canselor, Ketua-ketua PTj, Bilik Fail, Bilik Kebal, Bilik Perkakasan ICT, Stor ICT, Bilik Kawalan CCTV dan Pusat Data. (a) Akses kepada kawasan larangan hanyalah kepada staf yang dibenarkan sahaja, (b) Pihak ketiga dan pengguna lain adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan, bantuan teknikal atau lawatan rasmi, dan mereka hendaklah diiringi oleh staf yang dibenarkan, sepanjang masa sehingga urusan di kawasan berkenaan selesai.	Semua

0502 Keselamatan Peralatan

Objektif:

Melindungi aset ICT UNIMAS dari kehilangan, kerosakan, kecurian serta gangguan kepada aset tersebut.

050201 Aset ICT

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah memahami dan mematuhi UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy, (b) Pengguna hendaklah menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna, (c) Pengguna bertanggungjawab sepenuhnya ke atas aset ICT masing-masing, (d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan, (e) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT, (f) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan aset ICT di bawah kawalannya, (g) Pengguna mesti memastikan perisian antivirus di komputer peribadi/riba mereka sentiasa aktif (*activated*) dan dikemas kini disamping melakukan imbasan ke atas media storan yang digunakan, (h) Penggunaan kata laluan untuk akses ke sistem operasi komputer adalah diwajibkan, (i) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran, (j) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS), (k) Semua aset ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan, (l) Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci,	Pengguna

(m)	Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai,	
(n)	Pengguna yang ingin membawa keluar aset ICT dari premis UNIMAS, perlu mengisi Borang Kebenaran Membawa Keluar/Masuk Harta Benda/Peralatan Hak Milik UNIMAS (Rujuk Lampiran 4), mendapat kelulusan Ketua PTj dan direkodkan bagi tujuan pemantauan,	
(o)	Sebarang kehilangan aset ICT hendaklah dilaporkan kepada Pegawai Aset dan diuruskan mengikut Tatacara Pengurusan Kehilangan Aset Alih dengan segera,	
(p)	Pengendalian aset ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa,	
(q)	Pengguna tidak dibenarkan memindahkan aset ICT dari lokasi asal tanpa kebenaran Ketua PTj atau memohon melalui sistem UNIMAS Support bagi perkakasan di Pusat Data,	
(r)	Sebarang kerosakan aset ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT melalui UNIMAS Support,	
(s)	Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik,	
(t)	Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* untuk aset ICT guna sama yang telah ditetapkan oleh Pentadbir Sistem ICT,	
(u)	Pengguna dilarang sama sekali menggunakan *default password,*	
(v)	Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja,	
(w)	Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat kecuali komputer pengguna yang diberikan kebenaran akses SSL VPN atau fungsi khas; dan	
(x)	Sebarang bentuk penyelewengan atau salah guna aset ICT hendaklah dilaporkan kepada ICTSO.	

050202 Media Storan	
Perkara	**Tanggungjawab**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Pengguna hendaklah sentiasa memantau dan memastikan data dan maklumat yang disimpan terutamanya pada media storan berpusat tidak melebihi kuota yang ditetapkan. Pengguna bertanggungjawab untuk mengarkib, menghapus atau mengambil tindakan yang bersesuaian mengikut keutamaan data dan maklumat masing-masing. Media storan yang mengandungi maklumat kritikal perlu mematuhi perkara-perkara seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat, (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja, (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan, (d) Semua media storan yang mengandungi maklumat sulit hendaklah diletakkan di tempat yang terkawal dan selamat, (e) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal dan selamat, (f) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data, (g) Semua media storan data yang hendak dilupus mestilah dihapuskan dengan teratur dan selamat; dan	Pengguna

(h) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	

050203 Media Perisian dan Aplikasi

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah memahami dan mematuhi UNIMAS ICT Usage Policy and UNIMAS ICT Governance Policy, (b) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan UNIMAS sepertimana dinyatakan pada UNIMAS ICT Usage Policy and UNIMAS ICT Governance Policy, (c) Sistem aplikasi untuk kegunaan dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak luar kecuali dengan kebenaran Pengarah ICT, (d) Lesen perisian (*activation code*) perlu disimpan berasingan daripada media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (e) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengguna

050204 Penyelenggaraan Perkakasan

Perkara	Tanggungjawab
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	Staf Pejabat Pembangunan, Pengurus ICT,

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar, (b) Memastikan perkakasan hanya boleh diselenggara oleh staf atau pihak yang dibenarkan sahaja, (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan, (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan, (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Pentadbir Sistem dan Pihak Ketiga.
050205 Perkakasan di Luar Premis	
Perkara	**Tanggungjawab**
Perkakasan yang dibawa keluar dari premis UNIMAS adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perkakasan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan perkakasan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
050206 Pelupusan Perkakasan ICT	

Perkara	Tanggungjawab
Semua aset alih ICT sama ada harta modal atau inventori milik UNIMAS boleh dilupuskan berdasarkan justifikasi berikut: (a) Tidak ekonomi untuk diperbaiki, (b) Usang/ *obsolete,* (c) Rosak dan tidak boleh digunakan, (d) Luput tempoh penggunaan, (e) Keupayaan aset tidak lagi di peringkat optimum, (f) Tiada alat ganti, (g) Ketiadaan pembekal, (h) Disyor selepas pemeriksaan aset, (i) Tidak lagi diperlukan oleh UNIMAS, (j) Perubahan teknologi; atau (k) Melebihi keperluan. Aset ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan UNIMAS. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degaussing* atau pembakaran, (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan, (c) Aset ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat, (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya,	Pengguna

(e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut, (f) Pegawai Aset bertanggungjawab memohon untuk melupus serta merekodkan butir–butir pelupusan menggunakan borang KEW.PA-17 (Rujuk Lampiran 7) dan seterusnya mengemaskini rekod pelupusan, (g) Pelupusan aset ICT hendaklah dilakukan secara berpusat dan mengikut Tatacara Pengurusan Aset Alih UNIMAS; dan (h) Pengguna adalah dilarang sama sekali daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana aset 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 *UPS* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di UNIMAS, * iv. Memindah keluar dari UNIMAS mana-mana aset ICT yang hendak dilupuskan, * v. Melupuskan sendiri aset ICT kerana kerja-kerja pelupusan di bawah tanggungjawab UNIMAS; dan vi. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan sekunder seperti *flash drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. Nota: * Pengecualian kepada Pentadbir Sistem ICT	
0503 Keselamatan Persekitaran	

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

050301 Kawalan Persekitaran

Perkara	Tanggungjawab
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan/atau aset ICT, semua cadangan sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Pembangunan dan/atau TAHODC. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pejabat dengan teliti, (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan, (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan, (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT, (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT, (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT,	Pengguna (tidak termasuk Pelajar)

(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; dan (h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	

050302 Bekalan Kuasa

Perkara	Tanggungjawab
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua aset ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada aset ICT, (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) atau penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* dan bilik perkakasan rangkaian supaya mendapat bekalan kuasa berterusan; dan (c) Semua bekalan kuasa peralatan sokongan bagi perkhidmatan kritikal hendaklah diperiksa dan diuji sekurang-kurangnya satu (1) kali setahun.	Staf Pejabat Pembangunan, ICTSO, Pengurus ICT dan Pentadbir Sistem.

050303 Kabel Data

Perkara	Tanggungjawab

Kabel data hendaklah dilindungi kerana ia boleh menyebabkan ancaman dan gangguan kepada capaian maklumat. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan, (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan, (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan.	ICTSO, Pengurus ICT dan Pentadbir Sistem
050304 Prosedur Kecemasan	
Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Panduan Kecemasan yang telah ditetapkan oleh Bahagian Keselamatan UNIMAS; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan UNIMAS.	Semua
0504 Keselamatan Dokumen	

Objektif: Melindungi maklumat UNIMAS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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 Pekeliling Perkhidmatan Bil 5/2007 Panduan Pengurusan Pejabat, (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur pada 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.	Pengguna yang bertanggung jawab dalam menguruskan fail dan Pentadbir Sistem.

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI
0601 Pengurusan Prosedur Operasi

Objektif:

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

060101 Pengendalian Prosedur

Perkara	Tanggungjawab
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 dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua (tidak termasuk Pelajar)

060102 Kawalan Perubahan

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pegawai Penyelia atau Pentadbir Sistem ICT yang berkenaan terlebih dahulu, (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi	Semua (tidak termasuk Pelajar)

kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan, (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT, (b) Tugas mewujud, memadam, mengemas kini, 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, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan* yang digunakan sebagai *production*. * Perkakasan fizikal atau maya	Pengurus ICT dan ICTSO
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	

Objektif:

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

060201 Perkhidmatan Penyampaian

Perkara	Tanggungjawab
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 dipantau, disemak semula dan disahkan; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua (tidak termasuk Pelajar)

0603 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan Kapasiti

Perkara	Tanggungjawab

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh staf berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Perancangan kapasiti adalah mengikut keselamatan berpandukan Arahan Teknologi Maklumat MAMPU Disember 2007 bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus ICT, Pentadbir Sistem, Pihak Ketiga dan ICTSO.
060302 Penerimaan Sistem	
Perkara	**Tanggungjawab**
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus ICT, Pentadbir Sistem, Pemilik Sistem, Pihak Ketiga dan ICTSO.
0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya	
060401 Perlindungan dari Perisian Berbahaya	

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat, (b) Pengecualian untuk pemasangan antivirus adalah terpakai untuk pelayan yang menggunakan OS yang kurang berisiko dengan virus atau pelayan yang akan mengalami impak negatif kesan daripada instalasi antivirus, (c) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa (rujuk UNIMAS ICT *Usage Policy* dan UNIMAS ICT *Governance Policy*), (d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya, (e) Mengimbas kandungan sistem bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat, (f) Memastikan konfigurasi antivirus yang dipasang membenarkan pengemaskinian *pattern* antivirus yang terkini, (g) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya, (h) Mengadakan kawalan kualiti ke atas aplikasi yang dibangunkan; dan (i) Memberi hebahan mengenai ancaman keselamatan ICT seperti serangan virus.	Semua

060402 Perlindungan dari *Mobile Code*

Perkara	Tanggungjawab

Penggunaan *mobile code* atau aturcara/skrip seperti *worm*, makro dan Active X yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua

0605 Pengurusan *Backup*

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

060501 *Backup & Recovery*

Perkara	Tanggungjawab
Bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau sebelum pemasangan versi terbaru, (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat, (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan, (d) Menyimpan *backup* mengikut tempoh-tempoh yang ditetapkan; dan	Semua

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

0606 Pengurusan Rangkaian

Objektif:
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan (Lapisan OSI dari 4 ke atas seperti *Firewall*, *Application Switches* dan DNS).

060601 Kawalan

Perkara	Tanggungjawab
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 hendaklah diasingkan dari tugasan yang lain untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan, (b) Perkakasan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan mengurangkan daripada risiko bencana, (c) Capaian kepada perkakasan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja, (d) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT, (e) Konfigurasi *firewall* sentiasa dikemas kini berdasarkan keperluan semasa dan salinan konfigurasi disimpan oleh Pentadbir Sistem,	ICTSO, Pengurus ICT dan Pentadbir Sistem.

(f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan UNIMAS, (g) Semua perisian *sniffer, network analyser* dan *hacking* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO, (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat UNIMAS, (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat laman web dan aktiviti atas talian yang dilarang, (j) Sebarang penyambungan rangkaian perlu merujuk kepada UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy; dan (k) Kemudahan bagi rangkaian tanpa wayar perlu dipastikan kawalan keselamatannya.	

0607 Pengurusan Media

Objektif:

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

060701 Penghantaran dan Pemindahan

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

060702 Keselamatan Sistem Dokumentasi

Perkara	Tanggungjawab
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 (kecuali dokumen elektronik yang ada kawalan capaian) semua aktiviti capaian dokumentasi sulit sedia ada.	Semua

0608 Pengurusan Pertukaran/Perkongsian Maklumat dan Perisian

Objektif:
Memastikan keselamatan pertukaran/ perkongsian maklumat dan perisian terjamin di dalam UNIMAS mahupun dengan agensi luar.

060801 Pertukaran/Perkongsian Maklumat dan Perisian

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi,	Semua

(b) Persetujuan pertukaran maklumat dan perisian perlu diwujudkan di antara dalaman UNIMAS atau dengan Pihak Ketiga, (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari UNIMAS; dan (d) Maklumat sulit yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya dengan menggunakan kata laluan. Kata laluan perlu dihantar melalui medium yang berbeza seperti *instant messaging*.	

060802 Pengurusan Mel Elektronik (E-mel)

Perkara	**Tanggungjawab**
Penggunaan e-mel di UNIMAS hendaklah dipantau secara berterusan oleh Pentadbir Sistem untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy dan mana-mana undang-undang bertulis yang berkuatkuasa.	Pentadbir Sistem

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)

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

060901 E-Dagang

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

060902 Maklumat Umum

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian, (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

0610 Pemantauan

Objektif:
Melaksanakan pemantauan ketersediaan perkhidmatan dan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pemantauan Aktiviti ICT

Perkara	Tanggungjawab
Pentadbir Sistem mestilah bertanggung jawab menyemak dan mengambil tindakan ke atas perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT UNIMAS, (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*), (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak, (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan, (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan, (f) Aktiviti instalasi dan penggunaan perisian yang membebankan lebar jalur (*bandwidth*) rangkaian, (g) Aktiviti penyalahgunaan akaun e-mel, (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem; dan (i) Pemantauan ketersediaan perkhidmatan.	Pengurus ICT dan Pentadbir Sistem

061002 Jejak Audit

Perkara	Tanggungjawab
Setiap sistem mestilah mempunyai jejak audit. 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 kritikal, (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 Pentadbir Sistem 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.	Pengurus ICT dan Pentadbir Sistem

061003 Log Sistem

Perkara	Tanggungjawab
Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan log sistem bagi merekodkan • aktiviti pentadbiran dan operator sistem	Pengurus ICT dan Pentadbir Sistem

• kesalahan, kesilapan dan/atau penyalahgunaan (b) Menyimpan log untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian, (c) Waktu *(Timestamp)* yang berkaitan dengan sistem pemprosesan maklumat dalam UNIMAS atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui; dan (d) Sistem merekod log dan maklumat log perlu dilindungi daripada diubahsuai atau capaian yang tidak dibenarkan.	

061004 Pemantauan Log

Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala, (b) Menyemak, memantau, menganalisa dan mengambil tindakan sewajarnya ke atas sebarang penemuan, (c) Menyemak sistem log bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (d) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada UNIMAS-CSIRT.	UNIMAS-CSIRT, Pengurus ICT dan Pentadbir Sistem

BIDANG 07 KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:
Mengawal capaian ke atas maklumat.

070101 Keperluan Kawalan Capaian

Perkara	Tanggungjawab
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.	Pengurus ICT, Pentadbir Sistem dan ICTSO

0702 Pengurusan Capaian Pengguna

Objektif:
Mengawal capaian pengguna ke atas aset ICT UNIMAS.

070201 Akaun Pengguna

Perkara	Tanggungjawab
Setiap pengguna bertanggungjawab ke atas capaian kepada sistem/aplikasi/aset ICT. Langkah-langkah berikut perlu dipatuhi bagi membolehkan aktiviti pengguna dijejaki:- (a) Pengguna hanya dibenarkan menggunakan akaun yang diizinkan oleh UNIMAS, (b) Akaun pengguna mestilah unik, tidak boleh dikongsi dan menggambarkan identiti pengguna (c) UNIMAS berhak menarik balik segala hak capaian pada bila-bila masa tanpa makluman awal. (d) Kebenaran daripada Pemilik Data adalah WAJIB bagi akaun pengguna yang memerlukan hak untuk view, *insert*, *update* dan *delete* data. (e) Pentadbir Sistem ICT mempunyai hak untuk menggantung atau menamatkan akaun pengguna atas sebab berikut, setelah menerima arahan dari pihak Pengurusan UNIMAS: i) Perubahan bidang tugas yang tidak lagi memerlukan hak capaian kepada sistem ii) Bersara iii) Tamat Perkhidmatan/Pengajian iv) Dikenakan tindakan tatatertib / diberhentikan	Semua dan Pentadbir Sistem

070202 Hak Capaian

Perkara	Tanggungjawab

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan berdasarkan keperluan skop tugas.	Pengurus ICT, Pentadbir Sistem, Pemilik Sistem dan ICTSO
070203 Pengurusan Kata Laluan	
Perkara	**Tanggungjawab**
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 UNIMAS seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi, tidak boleh dikongsi dan tidak didedahkan dengan apa cara sekalipun, (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi, (c) Panjang kata laluan hendaklah sekurang-kurangnya lapan (8) aksara dengan kombinasi tiga daripada yang berikut; i) huruf besar ii) huruf kecil iii) simbol iv) nombor (d) Kata laluan komputer dan *screen saver/screen lock* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama, (e) Kata laluan komputer dan *screen saver/screen lock* hendaklah diaktifkan terutamanya pada komputer yang tidak join domain (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan (*hard coded*) di dalam program,	Semua dan Pentadbir Sistem

(g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula, (h) Pengguna digalakkan untuk menukar kata laluan secara berkala, (i) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna, (j) Kitar semula kata laluan adalah tidak dibenarkan, (k) Had masa sesi adalah mengikut kesesuaian sistem, (l) Klausa (a) dan (d) adalah terkecuali bagi komputer kegunaan umum; dan (m) Semua klausa di atas adalah terkecuali bagi sistem yang tidak menggunapakai UNIMAS Identity. Namun, sistem tersebut hendaklah mengadakan pengurusan kata laluan tersendiri.	

070204 *Clear Desk* dan *Clear Screen*

Perkara	**Tanggungjawab**
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 sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Menggunakan kemudahan *password screen saver/screen lock* atau *logout* apabila meninggalkan komputer, (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faks dan mesin fotostat.	

0703 Kawalan Capaian Rangkaian

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

070301 Capaian Rangkaian

Perkara	Tanggungjawab
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Memastikan pengguna membuat capaian pada sistem yang dibenarkan sahaja, (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. (d) UNIMAS mempunyai hak untuk memantau capaian elektronik sistem maklumat dalam semua aspek bagi mengelakkan sebarang kegagalan terhadap pematuhan polisi/peraturan UNIMAS.	Pengurus ICT, Pentadbir Sistem dan ICTSO

070302 Capaian Internet

Perkara	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di UNIMAS 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 UNIMAS, (b) Kaedah *content filtering* mestilah digunakan bagi mengawal akses Internet, (c) Penggunaan teknologi (*bandwidth management*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan lebar jalur (*bandwidth*) yang maksimum dan lebih berkesan, (d) Penggunaan Internet adalah untuk kegunaan rasmi namun kegunaan lain perlu dipastikan adalah pada tahap minima, (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 Ketua PTj sebelum dimuat naik ke Internet untuk capaian umum, (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 UNIMAS, (i) Penggunaan *switch/unauthorized devices* untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali. Rujuk	Pengurus ICT, Pentadbir Sistem dan ICTSO

	UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy; dan	
(j)	Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik/ turun, menyimpan dan menggunakan perisian tidak berlesen, sebarang aplikasi dan aktiviti yang boleh memberikan implikasi yang memudaratkan sistem rangkaian ICT UNIMAS seperti permainan elektronik, video dan *streaming*; dan ii. Menyedia, memuat naik/ turun dan menyimpan material, teks ucapan atau bahan-bahan sulit atau yang mengandungi unsur-unsur terlarang berdasarkan perundangan Malaysia.	

0704 Kawalan Capaian Sistem Pengoperasian

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

070401 Capaian Sistem Pengoperasian

Perkara	Tanggungjawab
Kawalan capaian sistem pengoperasian adalah perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:	Pengurus ICT, Pentadbir Sistem dan ICTSO

(a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan, (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *logon*, (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja, (c) Mengehadkan dan mengawal dengan rapi penggunaan utiliti atau program yang boleh memberi ancaman kepada sistem dan aplikasi; dan (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	

070501 Capaian Aplikasi dan Maklumat

Perkara	Tanggungjawab
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan, (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*system log*), (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (d) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah terhad kepada perkhidmatan yang dibenarkan sahaja.	Pengurus ICT, Pemilik Sistem, Pentadbir Sistem dan ICTSO

0706 Peralatan Mudah Alih dan Kerja di Luar Pejabat

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja di luar pejabat.

070601 Peralatan Mudah Alih

Perkara	Tanggungjawab

Bagi memastikan maklumat yang disimpan di dalam peralatan mudah alih dikawal dan dilindungi dengan rapi, perkara yang perlu dipatuhi termasuk yang berikut: (a) Peralatan mudah alih mesti disimpan di persekitaran yang selamat dan berkunci. (b) Peralatan mudah alih mesti berada pada kawalan visual pada setiap masa, terutamanya semasa berada di luar pejabat. (c) Semasa berada di kawasan umum atau gunasama, akses kepada data sulit hendaklah dihadkan. Sekiranya masih ada keperluan untuk berbuat demikian, maka langkah-langkah keselamatan, hendaklah diambil supaya data tersebut tidak boleh dilihat oleh pihak yang tidak berkenaan. (d) Peralatan mudah alih hendaklah dilengkapkan dengan sistem pengoperasian dan perisian antivirus yang telah diselenggarakan dengan baik. (e) Data sulit tidak dibenarkan untuk disimpan di dalam peralatan mudah alih. Namun dalam keadaan di mana tiada alternatif untuk penyimpanan data tersebut ke media storan berpusat, data sulit pada peralatan mudah alih mesti dilindungi melalui kaedah *data encryption* atau *personal firewall*. (f) Apabila data sulit tidak lagi perlu disimpan pada peralatan mudah alih, maka data tersebut hendaklah dihapuskan. (g) Proses *backup* perlu dilaksanakan bagi menjamin keselamatan data.	Semua
070602 Bring Your Own Device (BYOD)	
Perkara	**Tanggungjawab**
(a) Pengguna BYOD adalah tertakluk kepada perkara-perkara seperti berikut:	Semua

i. Bertanggungjawab menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuatkuasa. ii. Bertanggungjawab memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar / ditamatkan perkhidmatan/bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan. iii. Bertanggungjawab menjaga kerahsiaan maklumat rasmi kerajaan dan/atau Universiti. iv. Bagi keperluan *event*, pihak ketiga hendaklah membuat permohonan rasmi secara bertulis untuk capaian rangkaian dalaman UNIMAS kepada pegawai yang bertanggungjawab terhadap aset ICT tersebut dan kelulusan adalah tertakluk kepada pegawai yang bertanggungjawab. v. Bagi keperluan *adhoc*, "open guest account" ada disediakan dengan capaian terhad. (b) Pengguna BYOD adalah DILARANG daripada melakukan perkara berikut: i. Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat Rasmi dan Terperingkat kepada pihak yang tidak dibenarkan. ii. Penggunaan BYOD untuk tujuan peribadi yang boleh menganggu produktiviti kerja. iii. Menjadikan BYOD sebagai *access point* kepada perkakasan ICT yang lain untuk capaian ke Internet tanpa kebenaran.	
070603 Kerja di Luar Pejabat	
Perkara	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Pengguna hendaklah mematuhi Perkara 070601 Peralatan Mudah Alih jika berkenaan. (b) Pihak ketiga hendaklah membuat permohonan rasmi secara bertulis untuk capaian kepada rangkaian dalaman UNIMAS kepada pegawai yang bertanggungjawab terhadap aset ICT tersebut dan kelulusan adalah tertakluk kepada pegawai yang bertanggungjawab.	

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
080101 Keperluan Keselamatan Sistem Maklumat	
Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat, (b) Ujian keselamatan hendaklah dijalankan ke atas; i) sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, ii) sistem pemprosesan untuk menentukan sama ada	Pengurus ICT, Pemilik Sistem, Pentadbir Sistem dan ICTSO

program berjalan dengan betul dan sempurna dan; iii) Sistem *output* untuk memastikan data yang telah diproses adalah tepat, (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
080102 Pengesahan Data Input dan Output	
Perkara	**Tanggungjawab**
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.	Pengurus ICT, Pemilik Sistem dan Pentadbir Sistem
0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	

Perkara	**Tanggungjawab**

Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat rahsia rasmi pada setiap masa.	Semua
080202 Pengurusan Infrastruktur Kunci Awam (*PKI*)	
Perkara	**Tanggungjawab**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengurus ICT, Pentadbir Sistem dan ICTSO.
0803 Keselamatan Sistem Fail	
Objektif: Memastikan supaya sistem fail dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Sistem Fail	
Perkara	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian sistem fail hanya boleh dilakukan oleh Pentadbir Sistem atau staf yang berkenaan dan mengikut prosedur yang telah ditetapkan, (b) Kod atau atur cara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji,	Pengurus ICT dan Pentadbir Sistem.

(c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan pengubahsuaian tanpa kebenaran, penghapusan dan kecurian, (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 Prosedur Kawalan Perubahan

Perkara	Tanggungjawab
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 pembekal, (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut	Pengurus ICT, Pemilik Sistem dan Pentadbir Sistem

keperluan sahaja; dan (d) Akses kepada kod sumber (*source code)* aplikasi dihadkan kepada pengguna yang diizinkan. (e) Menghalang sebarang peluang untuk membocorkan maklumat.	

080402 Pembangunan Perisian Secara *Outsource*

Perkara	Tanggungjawab
Pembangunan perisian secara *outsource* perlu diselia dan dipantau. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik UNIMAS tertakluk kepada kontrak perjanjian.	Pihak Ketiga, CTO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pemilik Sistem.

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

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

080501 Kawalan dari Ancaman Teknikal

Perkara	Tanggungjawab
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 mengenalpasti tahap risiko yang	Pengurus ICT, Pentadbir Sistem dan ICTSO

bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN MAKLUMAT	
0901 Mekanisme Pelaporan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan maklumat.	
090101 Mekanisme Pelaporan	
Perkara	**Tanggungjawab**
Insiden keselamatan maklumat bermaksud musibah (*adverse event*) yang berlaku ke atas maklumat atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan maklumat yang telah ditetapkan. Insiden keselamatan maklumat yang melibatkan ICT seperti (a) hingga (e) hendaklah dilaporkan kepada ICTSO dan UNIMAS-CSIRT, manakala insiden keselamatan maklumat yang tidak melibatkan ICT seperti (a) hingga (b) hendaklah dilaporkan kepada Bahagian Keselamatan, 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,	Semua

(b) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka, (c) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian, (d) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; dan (e) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersasar. Prosedur pelaporan insiden keselamatan maklumat di UNIMAS adalah berdasarkan: (a) Pekeliling Am Bilangan 4 Tahun 2022 : Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam , (b) Bab F: Kehilangan dan Hapus Kira (Tatacara Pengurusan Aset Alih UNIMAS), bagi maklumat yang tidak melibatkan ICT; atau (c) SOP 1/18 Pencerobohan, Bahagian Keselamatan, (Rujuk Lampiran 2).	
0902 Pengurusan Maklumat Insiden Keselamatan Maklumat	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan maklumat.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan	
Perkara	**Tanggungjawab**

Maklumat mengenai insiden keselamatan 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 UNIMAS. Bahan-bahan bukti berkaitan insiden keselamatan maklumat hendaklah disimpan dan diselenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti, (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan, (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan, (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	Semua dan UNIMAS-CSIRT

BIDANG 10 PEMATUHAN
1001 Pematuhan dan Keperluan Perundangan
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKICT UNIMAS.

100101 Pematuhan Dasar

Perkara	Tanggungjawab
Setiap pengguna di UNIMAS hendaklah membaca, memahami dan mematuhi DKICT UNIMAS dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di UNIMAS termasuk maklumat yang disimpan di dalamnya adalah hak milik UNIMAS. Staf yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang pengguna aset ICT UNIMAS selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber UNIMAS.	Semua

100102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

100103 Pematuhan Keperluan Audit

Perkara	Tanggungjawab
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses sistem operasi maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

100104 Keperluan Perundangan

Perkara	Tanggungjawab
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di UNIMAS: (a) Arahan Keselamatan, (b) Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam, (c) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan, (d) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002; (e) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam, (f) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network)* di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006,	Semua

(g) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK), (h) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender, (i) Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan, (j) Akta Tandatangan Digital 1997, (k) Akta Rahsia Rasmi 1972, (l) Akta Jenayah Komputer 1997, (m) Akta Hak Cipta (Pindaan) Tahun 1997, (n) Akta Komunikasi dan Multimedia 1998, (o) Perintah-Perintah Am, (p) Arahan Perbendaharaan, (q) Arahan Teknologi Maklumat 2007; dan *(r)* UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy	
100105 Pelanggaran Dasar	
Perkara	**Tanggungjawab**
Pelanggaran **Dasar Keselamatan ICT (DKICT) UNIMAS**, UNIMAS ICT Usage Policy dan UNIMAS ICT Governance Policy, boleh dikenakan tindakan tatatertib.	Semua

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, *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 antara cakera keras d69omputerter) dalam jangka masa yang ditetapkan.
SQRC	*Strategic Planning, Quality and Risk Centre*
BYOD	Peralatan mudah alih persendirian seperti telefon pintar, tablet dan laptop yang digunakan untuk tujuan rasmi
Denial Services	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*).
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).
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaianrangkaian tersebut agar sentiasa berasingan.

GLOSARI	
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	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.
Media	Peralatan atau perantara yang digunakan untuk menyimpan data dan maklumat.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi–fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pemilik Proses	Pihak yang memiliki dan berhak ke atas maklumat tersebut.
Pengurusan UNIMAS	Pihak yang terlibat dalam membuat keputusan ke atas pengurusan pentadbiran UNIMAS.
Peralatan Mudah Alih	Komputer, komputer riba, tablet, telefon bimbit, dan peralatan milik UNIMAS yang menyimpan data dan menggunakan sistem rangkaian. Juga merangkumi kemudahan yang diuruskan atau dibekalkan oleh pihak ketiga melalui kontrak atau perjanjian.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
PTj	Pusat Tanggungjawab UNIMAS.
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, capaian Internet.

GLOSARI	
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switch	*Switch* merupakan alat yang boleh menapis dan menghantar paket data di antara segmen rangkaian.
Threat	Gangguan dan ancaman melalui pelbagai cara yang membahayakan dan boleh mengakibatkan kerosakan dan kerugian kepada UNIMAS.
Uninterruptible Power Supply (UPS)	Peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan ketika ketiadaan bekalan kuasa.
Video Conference	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Video Streaming	Penghantaran kandungan multimedia secara dalam talian menerusi aliran data berterusan tanpa pengguna perlu memuat-turun *file* terlebih dahulu untuk memainkannya.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi serta menjejaskan sistem rangkaian.
Wireless LAN	Rangkaian komputer yang terhubung tanpa wayar.
NACSA	National Cyber Security Agency
TAHODC	Tun Abang Haji Openg Digital Centre
KPT	Kementerian Pengajian Tinggi
OSHA	*Occupational Safety and Health Administration*
JSKU	Jawatankuasa Strategi dan Kualiti UNIMAS

Lampiran 1: Surat Akuan Pematuhan Dasar Keselamatan ICT UNIMAS

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT UNIMAS

Nama (Huruf Besar) :

.....

No. Kad Pengenalan :

.....

Jawatan :

.....

Nama Syarikat :

.....

No Pendaftaran Syarikat :

.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya atau mana-mana individu yang mewakili syarikat ini telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT UNIMAS dan apa-apa arahan yang dikuatkuasakan oleh Universiti Malaysia Sarawak dari masa ke semasa;

2. Saya atau mana-mana individu yang mewakili syarikat ini bertanggungjawab memastikan Dasar Keselamatan ICT UNIMAS difahami dan dipatuhi oleh semua individu di dalam syarikat ini yang berurusan dengan Universiti Malaysia Sarawak; dan
3. Jika saya atau mana-mana individu yang mewakili syarikat ini ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas saya atau mana-mana individu yang mewakili syarikat ini atau syarikat yang saya wakili.

Tanda tangan **: .....**

Tarikh **: .....**

Pengesahan Pegawai Keselamatan ICT

.....

( )

Tarikh: **.....**

Lampiran 2: Bahagian Keselamatan UNIMAS (S.O.P 1/18)

FUNGSI	**:**	**KAWALAN KESELAMATAN**
UNIT	**:**	**KESELAMATAN**
AKTIVITI	**:**	**PENCEROBOHAN**

Bil.	Prosedur Tetap Operasi	Tanggungjawab	Peraturan Dan Undang - undang
1	Terima maklumat berkaitan dengan pencerobohan di dalam bangunan/ kawasan universiti	Penyelia	
2	Pergi ke tempat kejadian dengan kadar segera	Penyelia	
3	Arahkan pasukan ronda ke tempat kejadian dan berkumpul di suatu tempat yang ditentukan	Penyelia	
	i) Bahagikan anggota untuk kawalan di setiap laluan keluar bangunan ii) Bentukkan satu pasukan pengesan iii) Pastikan setiap pasukan mempunyai alat komunikasi iv) Maklumkan Pos kawalan keselamatan tentang pencerobohan v) Mohon bantuan bilik kawalan CCTV untuk mengesan suspek	Rujuk Arahan Kerja	
4	Arahkan semua anggota untuk bertindak dengan kadar segera	Penyelia	

Bil.	Prosedur Tetap Operasi	Tanggungjawab	Peraturan Dan Undang - undang
5	Minta semua pasukan membuat laporan keadaan semasa	Penyelia	
6	Sekiranya penceroboh berjaya ditahan i) Ambil maklumat berkaitan dengan penceroboh ii) Rampas harta benda Universiti yang diambil iii) Hubungi Pihak Polis	Penyelia	
7	Sediakan anggota untuk memberi tunjuk arah dan iringi pihak Polis ke tempat kejadian	Penyelia/ Pengawal Keselamatan	
8	Jangan tinggal tempat kejadian	Penyelia	
9	Beri bantuan sepenuhnya kepada pihak Polis	Penyelia	
10	Sediakan laporan dan hantar ke Pejabat Keselamatan	Penyelia	

Lampiran 3: Borang Kebenaran Membawa Keluar/Masuk Harta Benda/Peralatan Hak Milik UNIMAS

UNIMAS/08.2.13

UNIVERSITI MALAYSIA SARAWAK
94300 KOTA SAMARAHAN

KEBENARAN MEMBAWA KELUAR/MASUK
HARTA BENDA/PERALATAN HAK MILIK UNIMAS

Kepada: Pengawal Keselamatan
Universiti Malaysia Sarawak

Butiran Pembawa

Nama: _____

F/I/B/P: _____

No. Staf/Matrik: _____ No. K/P: _____

Diskripsi Harta Benda/Peralatan Universiti

Bil.	Jenama & Model	No. Siri	Kuantiti
1.			
2.			
3.			
4.			
5.			

Adalah saya dengan ini mengaku membawa keluar harta benda/peralatan hak milik UNIMAS untuk tujuan berikut:

.....

.....

.....
Cop Jawatan dan Tandatangan

Pengesahan PTj : (Dekan/Pengarah/Pen. Pendaftar/Pegawai Bertanggungjawab)

.....
Tarikh dan Masa

.....
Cop Jawatan dan Tandatangan

(Nota: Borang ini hendaklah dilengkapkan sebelum membawa harta benda/peralatan keluar dari F/I/B/P)

1

Pindaan september 2013

UNIMAS/08.2.13

Untuk Tindakan Pengawal Keselamatan Pintu Keluar

Pemeriksaan dan Pengesahan Harta Benda/Peralatan Yang Di Bawa Keluar

Catatan:

....

Tarikh dan Masa Nama dan Tandatangan

Untuk Tindakan Pengawal Keselamatan Pintu Masuk

Pemeriksaan dan Pengesahan Harta Benda/Peralatan Yang Di Bawa Masuk

Catatan:

....

Tarikh dan masa Nama dan Tandatangan

(Nota: Bahagian Catatan diisi dengan maklumat status pemeriksaan dan pengesahan hartabenda/peralatan yang dibawa keluar dan masuk)

2

Lampiran 4: KEW.PA-2 Daftar Harta Modal

(KEW.PA-2)

UNIVERSITI MALAYSIA SARAWAK
DAFTAR HARTA MODAL

FAKULTI/INSTITUT/PUSAT/BAHAGIAN : /
NO PENDAFTARAN ASET :
TAG ASET :

BAHAGIAN A

Nama Aset			
Kategori			
Kelas Aset			
Jenis/Jenama/Model		**Harga Asal**	RM
Buatan		**Tarikh terima**	
Jenis & No.Enjin		**No Pesanan Belian**	
No. Casis/ Siri Pembuat		**Tempoh Jaminan**	
No. Pendaftaran (Bagi Kenderaan)		**Nama Pembekal & Alamat:**	
Vot Peruntukan	/ / /		
Komponen/Aksesori :		..... **Tandatangan Ketua Pusat Tanggungjawab** **Nama:** **Jawatan:** **Tarikh:** **Cop Rasmi:**	

PENEMPATAN

Lokasi:						
Tarikh:						
Nama Pegawai :						
Tandatangan :						

PEMERIKSAAN

Tarikh :						
Status Aset: :						
Nama Pemeriksa:						
Tandatangan:						

PELUPUSAN/HAPUS KIRA

Rujukan Kelulusan	Tarikh	Kaedah Pelupusan	Tandatangan

PEJABAT BURSAR, UNIVERSITI MALAYSIA SARAWAK

(KEW.PA 2)

UNIVERSITI MALAYSIA SARAWAK

DAFTAR HARTA MODAL
BUTIR-BUTIR PENAMBAHAN, PENGGANTIAN DAN NAIK TARAF

BAHAGIAN B

BIL	TARIKH	BUTIRAN	TEMPOH JAMINAN	KOS (RM)	NAMA DAN TANDATANGAN

PEJABAT BENDAHARI, UNIVERSITI MALAYSIA SARAWAK KEW.PA-2 BAHAGIAN B

Lampiran 5: KEW.PA-3 Daftar Inventori

(KEW.PA-3)

DAFTAR INVENTORI

UNIVERSITI MALAYSIA SARAWAK

FAKULTI/INSTITUT/PUSAT/BAHAGIAN : ( )
NO PENDAFTARAN INVENTORI :

Nama Item			
Kategori			
Kelas			
Model /Jenama	/	**Harga Asal**	RM
Kuantiti	1	**Tarikh terima**	
Unit Pengukuran		**No Pesanan Belian**	
No Siri		**No Pesanan Belian**	
Vot Peruntukan	/		
Nama Pembekal : (**Alamat**) **Pembekal/Syarikat:** **No. Telefon:**		..... **Tandatangan** **Ketua Pusat Tanggungjawab** **Nama:** **Jawatan:** **Tarikh:** **Cop Rasmi:**	

PENEMPATAN

Lokasi:						
Tarikh:						
Nama Pegawai :						
Tandatangan :						

PEMERIKSAAN

Tarikh :						
Status Inventori: :						
Nama Pemeriksa:						
Tandatangan:						

PELUPUSAN/HAPUS KIRA

Tarikh	Rujukan	Kaedah Pelupusan	Kuantiti	Lokasi	Tandatangan

PEJABAT BURSAR, UNIVERSITI MALAYSIA SARAWAK

Lampiran 6: KEW.PA-17 Permohonan/Laporan Jawatankuasa Pemeriksa Pelupusan Aset Alih

KEW.PA-17

UNIVERSITI MALAYSIA SARAWAK

PERMOHONAN/LAPORAN JAWATANKUASA PEMERIKSA PELUPUSAN ASET ALIH

(Maklumat Aset hendaklah diisi oleh Pusat Tanggungjawab dengan lengkap dalam ruangan yang disediakan)

Pusat Tanggungjawab: .....

BIL	KETERANGAN ASET	UNIT	KUANTITI	TARIKH PEMBELIAN (INVOIS)	TEMPOH DIGUNAKAN / SIMPANAN	HARGA PEROLEHAN ASAL		NILAI SEMASA		NYATAKAN KEADAAN ASET DENGAN JELAS	SYOR KAEDAH PELUPUSAN DAN JUSTIFIKASI (Untuk kegunaan Pemeriksa)
						SEUNIT (RM)	JUMLAH (RM)	SEUNIT (RM)	JUMLAH (RM)		
					JUMLAH KESELURUHAN						

Tarikh Pelantikan Jawatankuasa Pemeriksa .....

Tarikh Pemeriksaan .....

Tempat Pemeriksaan .....

Tandatangan .....(Pengerusi)
Nama .....
Jawatan .....

Tandatangan .....(Ahli)
Nama .....
Jawatan .....

Tandatangan .....(Ahli)
Nama .....
Jawatan .....

Tandatangan .....(Ahli)
Nama .....
Jawatan .....

Nota:
1. Sila lampirkan KEW PA-2/KEW PA-3
2. Gunakan lampiran 1/KEW PA-17 sekiranya ruangan tidak mencukupi
3. Borang ini hendaklah dihantar dan dicetak menggunakan kertas berwarna seperti berikut:-
(a) Pelupusan berkaitan ICT (dihantar kepada PKTMK) - BIRU
(b) Pelupusan bukan ICT (dihantar kepada BPA) - HIJAU