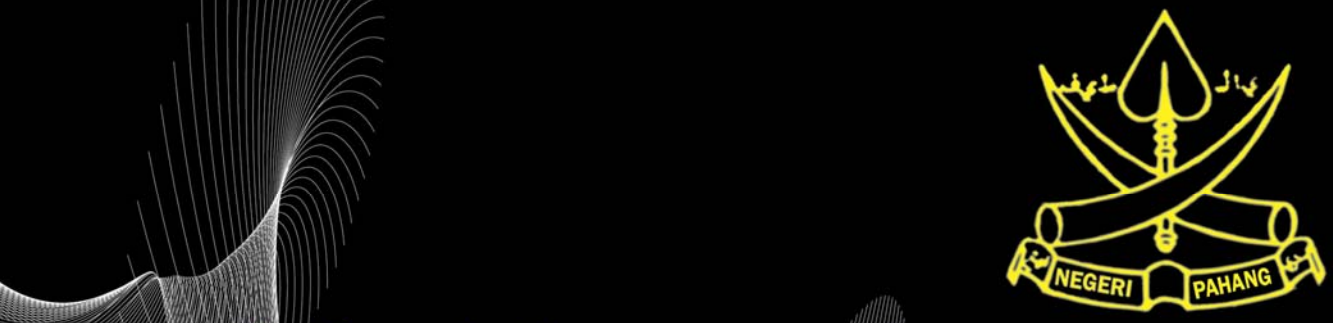


مجلس اڬام اسلام دان عادة رسم ملايو فهڠ

MAJLIS UGAMA ISLAM DAN ADAT RESAM MELAYU PAHANG

DASAR ICT MUIP

WWW.MUIP.GOV.MY

KANDUNGAN

DASAR ICT MAJLIS UGAMA ISLAM DAN ADAT RESAM MELAYU PAHANG (MUIP)

BAB 1
DASAR UMUM TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

1.1 Tujuan Dasar

Dasar ini menerangkan secara umum dasar penggunaan sumber-sumber Teknologi Maklumat dan Komunikasi (ICT) yang terdapat di Majlis Ugama Islam Dan Adat Resam Melayu Pahang (MUIP) dan diterima pakai sebagai Dasar Umum. Mana-mana dasar terperinci untuk setiap sumber yang disenarai adalah mengatasi Dasar Umum ini.

1.2 Objektif Dasar

Penggunaan ICT oleh staf MUIP adalah merupakan suatu peranan penting dalam mencapai misi dan visi MUIP. Dasar ini bertujuan memastikan :

i. warga MUIP dimaklumkan mengenai kewujudan dan peranan dasar-dasar ICT MUIP;
ii. kemudahan ICT digunakan secara bijaksana mengikut dasar yang ditetapkan;
iii. tanggungjawab pengguna dimaklumkan; dan
iv. kerosakan, kemusnahan dan penyalahgunaan ICT dapat diminimumkan.

1.3 Skop Dasar

1.3.1 Sumber

Sumber-sumber yang tersenarai di dalam dokumen, juga sumber-sumber yang tidak tersenarai tetapi dianggap sebagai sumber ICT adalah juga tertakluk kepada dasar ini.

1.3.2 Pengguna

Semua pengguna adalah tertakluk kepada dasar ini. Sesiapa yang tidak diberi kebenaran adalah dianggap sebagai penceroboh, dan boleh diambil tindakan yang sesuai mengikut kesalahan yang dilakukan, sebagaimana yang disebut dalam Dasar Penggunaan Teknologi Maklumat dan Komunikasi, MUIP.

1.4 Definisi

Definisi-definisi berikut digunakan dalam Penyataan Dasar yang berkaitan dengan penggunaan kemudahan ICT MUIP :

i. “MUIP” atau “Majlis” bermaksud Majlis Ugama Islam Dan Adat Resam Melayu Pahang;
ii. “staf” bermaksud sebagai seseorang yang dilantik oleh MUIP untuk sesuatu jawatan sama ada secara tetap, sambilan, sementara atau kontrak dan masih berkhidmat dengan MUIP;
iii. “kemudahan ICT” termasuk, tetapi tidak terhad kepada, sistem komputer peribadi, terminal, sistem komputer, alat-alat pinggiran komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, pembekalan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada MUIP. Ia termasuk semua kemudahan yang

disediakan oleh MUIP secara terpusat dan yang disediakan melalui Unit;

iv. “perisian” bermaksud aturcara atau program yang digunakan untuk melaksanakan tugas tertentu oleh komputer seperti perisian automasi pejabat, grafik dan sebagainya;

v. “aplikasi” bermaksud aturcara atau program yang dibangunkan untuk melaksanakan tugas tertentu oleh komputer seperti Sistem Maklumat Agihan Zakat, Sistem Maklumat Muallaf dan sebagainya;

vi. “perkakasan” bermaksud peralatan dan komponen ICT seperti komputer, notebook, pencetak dan sebagainya;

vii. “komputer server” bermaksud komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat;

viii. “peralatan rangkaian” bermaksud peralatan dan komponen yang digunakan dalam sistem rangkaian seperti switch, hub, router dan sebagainya;

ix. “pengguna” bermaksud seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT MUIP;

x. “tugas-tugas dalaman” bermaksud tugas-tugas yang menyokong fungsi-fungsi MUIP;

xi. “tugas luar” bermaksud tugas-tugas selain dari tugas dalaman;

xii. “maklumat peribadi" merujuk kepada data atau maklumat tentang seseorang individu, termasuk nama, tarikh lahir dan sebagainya; yang mana data-data ini boleh digunakan untuk mengenali seseorang individu contohnya nombor kad pengenalan, nombor staf dan sebagainya;

xiii. "pengurus" merujuk kepada seseorang yang dilantik dan diberi kuasa (authority) oleh majlis untuk mengendali, mengurus, menyelenggara dan menjaga kerahsiaan dan keselamatan maklumat majlis;

xiv. "tuan punya maklumat" merujuk kepada seseorang individu yang boleh dikenal pasti melalui maklumat peribadi yang ada;

xv. “akaun pengguna” merujuk kepada ruang storan yang telah diperuntukkan kepada setiap pengguna yang sah dalam sesuatu sistem atau sumber ICT. Setiap pengguna dikenalpasti melalui penggunaan identiti pengguna;

xvi. “maklumat rahsia” atau “sulit” dalam dokumen ini merujuk kepada segala bentuk data sama ada teks, grafik, audio, animasi dalam pelbagai format sama ada yang boleh dicerna seperti teks ataupun dalam format binari yang terdapat dalam akaun pengguna. Maklumat ini juga boleh dicapai semasa dalam medium penghantaran (transmisi) seperti data e-mel dalam talian atau dalam simpanan fail sementara;

xvii. “aktiviti” atau “kegiatan sulit” atau “rahsia pengguna” merujuk kepada arahan-arahan yang dilaksanakan (run) atau ‘keystrokes’ yang ditaip semasa pengguna berinteraksi dengan sumber IT yang disediakan oleh MUIP; dan

xviii. “pentadbir rangkaian” bermaksud pegawai yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian MUIP.

1.5 Dasar Am

i. Majlis bertanggungjawab menyediakan kemudahan ICT bagi kegunaan kakitangan bagi menyokong fungsi majlis.

ii. Semua kemudahan dan perkhidmatan ICT yang disediakan oleh MUIP adalah hak mutlak MUIP. Pengguna berdaftar diberikan keistimewaan untuk menggunakan kemudahan tersebut berdasarkan keperluan tugas dan bukannya hak yang diberikan kepada pengguna. MUIP berhak menarik balik kebenaran dan/atau kemudahan yang diberikan pada bila-bila masa tanpa notis.

iii. Kemudahan ICT yang disediakan oleh MUIP hanya boleh digunakan untuk tujuan yang berkaitan dengan fungsi MUIP. Penggunaan selain daripada yang berkaitan dengan fungsi MUIP adalah tidak dibenarkan, seperti untuk tujuan peribadi, komersil dan politik.

iv. Pengguna yang menggunakan peralatan ICT peribadi yang dibenarkan di dalam pejabat juga tertakluk kepada dasar ini. Sebarang penggunaan adalah tertakluk kepada undang-undang dan dasar MUIP, negeri dan negara. MUIP tidak akan bertanggungjawab terhadap sebarang penyalahgunaan yang dilakukan oleh pengguna.

v. Setiap pengguna mesti mematuhi Dasar ICT yang ditetapkan selaras dengan hasrat MUIP mewujud pengguna yang beretika dan menghormati pengguna yang lain.

vi. Majlis bertanggungjawab memastikan pelaksanaan Dasar ICT dan syarat-syarat yang berkaitan dengan pengguna dan kod etika diamalkan selaras dengan kemudahan-kemudahan di bawah kawalan majlis.

vii. Ketua-ketua Unit bertanggungjawab memastikan Dasar ICT diamalkan selaras dengan kemudahan-kemudahan di bawah kawalan dan pengurusannya.

viii. Dasar ini adalah tertakluk kepada perubahan dari semasa ke semasa. MUIP berhak meminda, membatal, menghad dan menambah mana-mana Dasar mengikut kesesuaian dan keperluan semasa.

1.6 Pelanggaran Dasar

i. Sebarang pelanggaran dasar dan peraturan oleh pengguna akan dikenakan tindakan berdasarkan kepada jenis pelanggaran dan keadaan semasa pelanggaran.

ii. Sebarang aduan tentang pelanggaran Dasar hendaklah dibuat secara bertulis kepada Jawatankuasa Keselamatan ICT MUIP. Jawatankuasa Keselamatan ICT boleh melantik Jawatankuasa Penyiasat untuk meneliti laporan dan boleh membuat keputusan sama ada siasatan terperinci perlu dilaksanakan.

iii. Tindakan atau penalti yang boleh dikenakan oleh Jawatankuasa Keselamatan ICT MUIP adalah penggantungan penggunaan kemudahan ICT. Lain-lain tindakan atau penalty boleh diambil oleh Jawatankuasa Tatatertib Staf untuk staf dengan mengikut prosidur yang ditetapkan.

1.7 Dasar Teknologi Maklumat Peringkat Kebangsaan

Dasar ini tidak terhad kepada kandungan dokumen ini, malah ia turut mencakupi serta menerimapakai dasar-dasar ICT peringkat kebangsaan seperti:

i. Dasar Pengurusan Keselamatan ICT Sektor Awam Malaysia berdasarkan Pekeliling Am Bil. 1 Tahun 2003 yang dikeluarkan oleh MAMPU;

ii. Garis Panduan Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-Agensi Kerajaan berdasarkan Pekeliling Am Bil.1 tahun 2003 yang dikeluarkan oleh MAMPU;

iii. Undang-undang Siber (Cyber Law) yang diperkenalkan oleh kerajaan di bawah program "MSC Bill of Guarantees" yang terdiri daripada akta-akta berikut:
   - Tandatangan Digital 1997
   - Hakcipta (amendment) 1997
   - Jenayah Komputer 1997
   - Tele-medicine 1997
   - Komunikasi dan Multimedia 1998
   - Suruhanjaya komunikasi dan Multimedia Malaysia 1998

BAB 2
DASAR PENGURUSAN ICT

2.1 Tujuan Dasar

Dasar ini menerangkan secara umum aspek pengurusan organisasi dan pembangunan Teknologi Maklumat dan Komunikasi (ICT) MUIP.

2.2 Skop Dasar

Skop dasar melibatkan :

i. aspek pengurusan organisasi ICT yang mempunyai kuasa dan kepakaran untuk merancang, melaksana dan mengurus keperluan ICT majlis menerusi strategi-strategi yang ditetapkan; dan
ii. aspek pembangunan ICT bagi merancang, mengurus, melaksana dan menyelenggara keperluan ICT Majlis menerusi strategi-strategi yang ditetapkan.

2.3 Dasar Pengurusan Organisasi

2.3.1 Penubuhan Jawatankuasa Teknikal ICT MUIP;

i. Menubuhkan jawatankuasa untuk menggubal dasar, arah tuju dan matlamat ICT MUIP
ii. Meluluskan perancangan ICT MUIP
i. Jawatankuasa ini dipengerusikan oleh Timbalan Yang Dipertua MUIP, Pegawai-Pegawai, Ketua Unit sebagai ahli dan keahlian lain adalah dilantik oleh pihak majlis.
iii. Staf Unit Teknologi Maklumat ialah urusetia bagi jawatankuasa ini.
ii. Jawatankuasa perlu mengadakan mesyuarat dari semasa ke semasa.

2.3.1 Penubuhan Unit Teknologi Maklumat;

i. Unit Teknologi Maklumat bertanggungjawab dalam merancang, melaksana, mengurus, memantau dan menyelenggara projek-projek ICT majlis.
ii. Unit mesti mempunyai staf yang mempunyai kepakaran ICT yang secukupnya.

2.3.2 Penubuhan Jawatankuasa Keselamatan ICT

iii. Jawatankuasa ditubuhkan untuk merancang pelaksanaan, pemantauan dan penguatkuasaan serta mengemaskini Dasar Keselamatan ICT.
iv. Jawatankuasa ini dipengerusikan oleh Timbalan Yang Dipertua MUIP, Pegawai-Pegawai, Ketua Unit sebagai ahli dan keahlian lain adalah dilantik oleh pihak majlis.
v. Staf Unit Teknologi Maklumat ialah urusetia bagi jawatankuasa ini.
vi. Jawatankuasa perlu mengadakan mesyuarat dari semasa ke semasa.

2.4 Dasar Pembangunan ICT

2.4.1 Perancangan ICT

i. Perancangan hendaklah memenuhi fungsi dan keperluan majlis.
ii. Perancangan hendaklah selaras dengan agenda ICT Negeri/Negara.
iii. Perancangan hendaklah mematuhi Dasar, Peraturan dan Garis Panduan yang ditentukan oleh pihak majlis.

2.4.2 Perolehan ICT

i. Semua perolehan hendaklah mematuhi Dasar Perolehan serta Kewangan majlis.
ii. Perolehan hendaklah memenuhi teknologi terkini dengan mendapat perakuan spesifikasi oleh Unit Teknologi Maklumat.
iii. Semua perisian aplikasi dan perisian sistem hendaklah mempunyai lesen yang sah.
iv. Semua pembangunan atau perolehan sistem aplikasi hendaklah dibuat melalui Unit Teknologi Maklumat bagi menjamin keseragaman, keserasian dan keselamatan sistem.

2.4.3 Instalasi dan Penyelenggaraan

i. Semua instalasi atau pemasangan perkakasan dan/atau perisian dilakukan di bawah penyeliaan Unit Teknologi Maklumat.

2.4.4 Naiktaraf atau Pelupusan

i. Semua naik taraf perkakasan dan perisian hendaklah mendapat kelulusan Unit Teknologi Maklumat.
ii. Perkakasan yang tidak berkeupayaan dan/atau tidak sesuai untuk dinaiktaraf atau diperbaiki boleh dicadang untuk pelupusan mengikut Prosidur Pelupusan majlis.

2.4.5 Pembangunan Sumber Manusia

i. Merancang keperluan sumber manusia yang secukupnya bagi menyokong perkhidmatan ICT majlis.
ii. Merancang, menyedia dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran teknikal ICT.
iii. Merancang, menyedia dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran asas ICT serta penggunaan aplikasi ICT majlis.

2.4.6 Keselamatan ICT

i. Semua pengguna hendaklah mematuhi :
    a. Dasar Penggunaan Bahan dan Perkakasan ICT;
    b. Dasar Keselamatan ICT majlis;
    c. Dasar Pengurusan Keselamatan ICT Sektor Awam Malaysia berdasarkan Pekeliling Am Bil. 1 Tahun 2003 yang dikeluarkan oleh MAMPU; dan
    d. Akta / Undang-Undang berkenaan yang digubal oleh Kerajaan Malaysia.

BAB 3
DASAR PERISIAN, APLIKASI DAN PERKAKASAN ICT

3.1 Tujuan Dasar

Dasar ini menentukan tanggungjawab pengguna dan pihak MUIP di dalam perkara-perkara yang berhubung dengan perisian, aplikasi dan perkakasan ICT majlis.

3.2 Skop Dasar

Skop dasar melibatkan :

i. semua perisian majlis yang dimiliki atau diguna atau berada di dalam simpanan pengguna tidak kira di mana perisian itu berada;
ii. semua aplikasi majlis yang dibangun atau diperolehi atau berada di dalam simpanan pengguna tidak kira di mana aplikasi itu berada; dan
iii. semua perkakasan majlis yang dimiliki atau diguna atau berada di dalam simpanan pengguna tidak kira di mana perkakasan itu berada.

3.3 Dasar Perisian dan Aplikasi

3.3.1 Hakmilik

i. Semua perisian dan aplikasi yang diperolehi untuk atau bagi pihak MUIP atau semua perisian yang dibangunkan oleh staf MUIP adalah menjadi hakmilik MUIP.
ii. Bagi perisian dan aplikasi yang dibangunkan, maklumat tentang semua pengarang / pencipta mestilah dikekalkan.
iii. Semua perisian dan aplikasi hakmilik MUIP tidak dibenarkan dijual, disewa, dilesenkan semula, dipinjam, disalin semula, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran majlis.

3.3.2 Perolehan

i. Semua perolehan perisian dan aplikasi hendaklah mengikut prosidur perolehan majlis.
ii. Semua perolehan perisian untuk kegunaan majlis hendaklah menggunakan versi terkini.
iii. Penggunaan adalah tertakluk kepada terma dan syarat penggunaan yang ditetapkan oleh pihak majlis, pembekal atau pembangun perisian.
iv. MUIP tidak akan bertanggungjawab terhadap sebarang perolehan dan penggunaan perisian tanpa lesen yang dilakukan oleh pengguna.
v. Majlis bertanggungjawab melaksanakan peningkatan dan naiktaraf perisian dan aplikasi bagi memastikan versi yang terkini digunapakai.
vi. Majlis bertanggungjawab menyediakan perkhidmatan penyelenggaraan bagi aplikasi yang memerlukan kepakaran khusus mengikut tempoh yang sesuai.
vii. Majlis menggalakkan penggunaan dan pembangunan aplikasi dan perisian sumber terbuka (OSS).

3.3.3 Tanggungjawab pengguna

i. Semua pengguna secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi dasar dan pelesenan bagi setiap perisian yang digunakan.
ii. Semua pengguna tidak dibenarkan memindah turun, membuat instalasi dan mengguna perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian MUIP misalnya perisian P2P (peer to peer) internet seperti Kazaa, iMesh, Morpheus, Grokster dan sebagainya.
iii. Semua pengguna tidak dibenarkan menyebar sebarang perisian berlesen secara tidak sah. Majlis tidak akan bertanggungjawab ke atas sebarang kesalahan yang dilakukan oleh pengguna.
iv. Sebarang bentuk permainan komputer tidak dibenarkan.

3.4 Dasar Perkakasan

3.4.1 Hakmilik

i. Semua perkakasan yang diperolehi untuk atau bagi pihak MUIP atau semua perkakasan yang dicipta atau dipasang mengguna peruntukan majlis oleh staf MUIP adalah menjadi hakmilik MUIP.
ii. Bagi perkakasan yang dicipta, maklumat tentang semua pencipta mestilah dikekalkan.
iii. Perkakasan tersebut tidak dibenarkan dijual, disewa, dipaten, dipinjam, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran majlis.

3.4.2 Perolehan Perkakasan

i. Semua perolehan perkakasan hendaklah mengikut prosidur perolehan majlis.
ii. Spesifikasi perkakasan hendaklah diperakukan oleh Unit Teknologi Maklumat MUIP bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa.
iii. Setiap perolehan perkakasan dimaklumkan kepada Unit Teknologi Maklumat untuk pengesahan spesifikasi perolehan dan tujuan rekod dan inventori majlis.

3.4.3 Pengagihan Perkakasan

i. Semua pengagihan perkakasan hendaklah mengikut prosidur majlis.
ii. Kakitangan Pengurusan dan Profesional – layak mendapat satu (1) unit PC atau notebook untuk setiap seorang. Kemudahan perkakasan daripada sumber-sumber lain tertakluk kepada kelulusan majlis. Peruntukan adalah berasaskan kekananan jawatan, beban tugas dan kesediaan peralatan.
iii. Kakitangan kategori lain – layak diberi PC berdasarkan keperluan kerja yang ditentukan oleh Ketua Jabatan/Unit. Sebarang permohonan individu atau berkumpulan hendaklah dibuat secara bertulis kepada Unit Teknologi Maklumat dengan mendapat perakuan Ketua Jabatan/Unit.
iv. Setiap pengguna hanya layak mendapat peruntukan satu PC atau notebook dalam satu-satu masa.

v. Kakitangan yang tamat perkhidmatan termasuk tetapi tidak terhad kepada bersara atau meletak jawatan, bercuti sabatikal luar negara atau melanjut pengajian, perlu memaklum dan memulang perkakasan di bawah tanggungjawabnya kepada Unit Teknologi Maklumat selewat-lewatnya satu (1) minggu sebelum tarikh berkaitan.

3.4.4 Peminjaman Perkakasan

i. Peminjam bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam.
ii. Peminjam perlu melapor dengan segera secara bertulis sekiranya berlaku kerosakan atau kehilangan perkakasan yang dipinjam kepada Unit Teknologi Maklumat untuk diambil tindakan yang sesuai.
iii. Peminjam perlu memulangkan perkakasan yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan.
iv. Peminjam perlu mengganti atau membayar kos perkakasan sekiranya berlaku kerosakan ke atas perkakasan yang dipinjam.
v. Tempoh pinjaman adalah tertakluk kepada kelulusan Unit Teknologi Maklumat melalui Ketua Jabatan/Unit.

3.4.5 Baik Pulih dan Penyelenggaraan Perkakasan

i. Semua baik pulih dan penyelenggaraan perkakasan hendaklah mengikut prosidur majlis.
ii. Bagi kerosakan perkakasan yang dibekalkan oleh Unit Teknologi Maklumat dikehendaki membuat aduan kepada Unit Teknologi Maklumat melalui saluran aduan yang disediakan misalnya Borang, Sistem atas talian atau telefon. Urusan pembaikan dan penyelenggaraan akan diurus sepenuhnya oleh Unit Teknologi Maklumat.
iii. Unit Teknologi Maklumat menyediakan perkhidmatan penyelenggaraan pencegahan.
iv. Majlis bertanggungjawab menyediakan perkhidmatan penyelenggaraan bagi perkakasan yang memerlukan kepakaran khusus mengikut tempoh yang sesuai.

3.4.6 Pelupusan Perkakasan

i. Semua perkakasan yang didapati tidak sesuai dinaik taraf atau diselenggara hendaklah dicadang dilupus mengikut prosidur Pelupusan majlis.
ii. Bagi perkakasan yang dibekalkan oleh Unit Teknologi Maklumat, Unit Teknologi Maklumat akan membuat cadangan pelupusan kepada Jawatankuasa Pelupusan MUIP.
iii. Mana-mana perkakasan yang dilupuskan akan diganti baru tertakluk kepada peruntukan majlis.

3.4.7 Tanggungjawab Pengguna

i. Pengguna tidak berhak mengganggu dengan apa cara sekalipun perkakasan yang bukan berada bawah kawalannya. Ini termasuk mengguna atau mengambil tanpa kebenaran, menceroboh dan mencuri perkakasan atau komponen-komponennya.

ii. Sebarang penggunaan secara perkongsian *(sharing)* adalah menjadi tanggungjawab bersama semua pengguna terbabit. Sebarang kongsian perlu mempunyai syarat dan dasar yang dipersetujui ahli (pengguna).

iii. Melapor segera secara bertulis kepada Unit Teknologi Maklumat sekiranya perkakasan tersebut rosak atau tidak berfungsi untuk tujuan pembaikan.

iv. Melaporkan segera secara bertulis kepada Unit Teknologi Maklumat sekiranya perkakasan tersebut hilang atau dicuri dan membuat laporan berdasarkan Peraturan MUIP.

BAB 4
DASAR RANGKAIAN ICT

4.1 Tujuan Dasar

Dasar ini menentukan penyediaan, penggunaan dan pengoperasian komputer server, perkhidmatan rangkaian MUIP dan penyambungan infrastruktur rangkaian.

4.2 Skop Dasar

Skop dasar adalah merangkumi :

i. Komputer Server

Merangkumi semua sistem komputer server (perkakasan dan perisian) yang dibangun atau disediakan untuk pengguna yang dibenarkan. Ini termasuk server aplikasi, server operasi rangkaian dan server kegunaan setempat (domain, fail server).

ii. Perkhidmatan Rangkaian MUIP

Merangkumi semua sumber rangkaian, termasuk tetapi tidak terhad kepada peralatan rangkaian seperti *hubs, switches* dan *routers*, perisian aplikasi rangkaian seperti *e-mail, web browser* dan *ftp*, konsep konfigurasi rangkaian seperti penggunaan alamat IP dan teknologi dan protokol rangkaian yang diguna seperti teknologi Gigabit dan protokol TCP/IP.

4.3 Komputer Server

4.3.1 Hakmilik

i. Semua komputer server yang diperolehi untuk atau bagi pihak MUIP adalah menjadi hakmilik MUIP.

4.3.2 Perolehan

i. Semua perolehan hendaklah mengikut prosidur perolehan majlis.
ii. Spesifikasi komputer server hendaklah diperakukan oleh Unit Teknologi Maklumat bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa.
iii. Setiap perolehan komputer server dimaklumkan kepada Unit Teknologi Maklumat untuk pengesahan spesifikasi perolehan dan tujuan rekod dan aset majlis.

4.3.3 Konfigurasi dan Operasi

i. Semua komputer server untuk kegunaan dalaman akan diberi alamat IP dalaman statik. Alamat IP global boleh dipertimbangkan oleh Unit Teknologi Maklumat (sebagai pentadbir alamat IP MUIP) bagi keperluan capaian fail daripada luar.
ii. Pentadbir sistem perlu memastikan keselamatan server daripada pencerobohan. Ini termasuk tetapi tidak terhad kepada membuat pemeriksaan ke atas proses tersembunyi *(hidden processes)*, 'daemons', mengemaskini perisian seperti emel dan laman web, dan mengenalpasti tahap capaian pengguna dan penggunaan komputer server.

iii. Komputer server untuk kegunaan lain tidak dibenarkan menggunakan rangkaian MUIP untuk mengelak gangguan rangkaian.
iv. Alamat IP tidak dibenarkan diubah sama sekali kecuali setelah mendapat kelulusan Unit Teknologi Maklumat.
v. Login dan kata laluan untuk id 'root' dan 'super-user' adalah bawah kawalan dan tanggungjawab pentadbir komputer server sepenuhnya.

4.4 Dasar Rangkaian MUIP

4.4.1 Hakmilik

i. Semua sumber rangkaian yang diperolehi untuk atau bagi pihak MUIP adalah menjadi hakmilik MUIP.

4.4.2 Perolehan

i. Semua perolehan sumber rangkaian hendaklah mengikut prosidur perolehan majlis.
ii. Perolehan peralatan rangkaian seperti router dan titik akses wayarles *(wireless access point)* oleh Unit adalah tidak dibenarkan kecuali dengan kelulusan Unit Teknologi Maklumat.

4.4.3 Kemudahan Rangkaian MUIP

i. Pengguna tidak dibenarkan dalam apa bentuk sekali pun mengganggu lain-lain pengguna MUIP, Internet dan sebarang rangkaian yang lain termasuk tetapi tidak terhad kepada menghantar maklumat rambang secara emel atau mesej atas talian *(on-line).*
ii. Pengguna tidak boleh memberi sumber rangkaian bawah jagaannya termasuk tetapi tidak terhad kepada nod rangkaian dan kad wayarles untuk diguna oleh orang lain walaupun kepada kakitangan MUIP tanpa mendapat kelulusan pentadbir rangkaian.
iii. Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti yang dilakukannya termasuk tetapi tidak terhad kepada stesen kerja, komputer peribadi atau PDA yang melibatkan atau melalui rangkaian MUIP termasuk akses ke Internet dan rangkaian-rangkaian yang lain.
iv. Mana-mana komputer yang menjadi sumber ancaman atau penyebaran virus akan disekat capaiannya ke rangkaian MUIP. Perkhidmatan akan ditutup sehingga komputer tersebut disahkan bebas dari ancaman virus.

4.4.4 Penyambungan Rangkaian

i. Kelulusan dari Unit Teknologi Maklumat perlu diperolehi untuk pembelian peralatan rangkaian dan penyambungan ke rangkaian MUIP. Konfigurasi penyambungan hendaklah dibuat oleh pembekal bawah pengawasan dan kawalan pentadbir rangkaian Unit Teknologi Maklumat.
ii. Sebarang penyambungan rangkaian ke MUIP yang tidak mendapat kebenaran dari Unit Teknologi Maklumat adalah

menyalahi peraturan dan Unit Teknologi Maklumat berhak memutuskan penyambungan tersebut. Tindakan susulan boleh diambil ke atas pengguna atas nasihat majlis.

BAB 5
DASAR PENGGUNAAN INTERNET / INTRANET

5.1 Tujuan Dasar

Dasar ini menentukan penggunaan perkhidmatan Internet/Intranet oleh pengguna bersesuaian sepertimana yang dikehendaki oleh MUIP. Dasar ini juga bertujuan melahirkan pengguna Internet yang beretika selaras dengan fungsi MUIP sebagai sebuah institusi badan kerajaan.

5.2 Skop Dasar

Skop dasar adalah merangkumi :

i. penggunaan kemudahan emel MUIP dan bukan MUIP. Dasar ini terbahagi kepada dua bahagian, iaitu Dasar Am dan Dasar Khusus Emel;
ii. pembangunan laman web di MUIP dan
iii. penggunaan Internet / Intranet termasuk tetapi tidak terhad kepada capaian sistem aplikasi majlis, portal majlis, laman web, pemindahan data atau maklumat dan perbincangan melalui 'list group' atau 'chat room'.

5.3 Dasar Emel

5.3.1 Dasar Am

i. Aktiviti *spamming* atau *mail-bombing* dan penyebaran emel dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman dan gangguan) kepada individu, *mailing list* atau *discussion group* sama ada di dalam rangkaian MUIP atau ke Internet adalah tidak dibenarkan.
ii. MUIP berhak memasang sebarang jenis perisian atau perkakasan penapisan emel dan virus ('email filter and anti virus') yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis menyekat atau menghapuskan mana-mana emel yang disyaki mengandungi virus atau berunsur 'spamming' daripada memasuki ke dalam server.
iii. MUIP tidak bertanggungjawab terhadap pengguna yang menjadi penghantar ('sender') atau penerima ('receiver') kepada sebarang emel yang berunsur 'spamming' atau penyebaran emel dengan kandungan tidak beretika.
iv. MUIP tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, data, kotak emel atau fail yang disimpan oleh pengguna di dalam stesen kerja atau server akibat daripada penggunaan perkhidmatan emel.
v. Sistem emel yang disediakan oleh majlis mestilah boleh menyediakan kemudahan untuk menukar kata laluan secara berkala (dicadangkan dibuat setiap 3 bulan oleh pengguna) bagi mengelakkan pencerobohan akaun.

5.3.2 Dasar Khusus

i. Kemudahan emel disediakan dan diberi kepada semua staf. Kemudahan emel juga boleh disediakan kepada organisasi atau persatuan rasmi MUIP melalui permohonan kepada Unit Teknologi Maklumat. Pengguna tidak dibenarkan untuk memohon penukaran alamat emel.

ii. Seseorang pengguna individu tidak dibenarkan untuk memohon dan /atau memiliki lebih daripada satu akaun atau alamat emel MUIP pada satu-satu masa.

iii. Setiap alamat emel yang disediakan adalah untuk kegunaan individu atau organisasi/persatuan berkenaan sahaja dan tidak boleh digunakan oleh pihak lain sama ada secara kebenaran atau tanpa kebenaran.

iv. Pengguna dilarang menggunakan kemudahan emel untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan dan undang-undang majlis dan negara.

v. Semua pengguna yang diberi kemudahan emel MUIP tidak dibenarkan mengguna emel luar (seperti hotmail, yahoo dan lain-lain) untuk tujuan rasmi. Pentadbir Rangkaian berhak menghalang penggunaan emel tersebut jika didapati memudarat dan membebankan rangkaian MUIP.

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

vii. Dari semasa ke semasa atas sebab-sebab keperluan audit, keselamatan dan penggunaan, pentadbir emel dengan kelulusan majlis berhak memeriksa dan melihat isi kandungan emel dan ruang storan pengguna-pengguna.

viii. Unit Teknologi Maklumat boleh menamatkan kemudahan akaun emel yang telah diberikan kepada staf atas sebab-sebab berikut :
   a. staf telah tamat atau ditamatkan perkhidmatan dengan MUIP secara rasmi;
   b. persatuan yang telah dibubar secara rasmi oleh majlis;
   c. permintaan dari staf sendiri untuk menamatkan perkhidmatan tersebut; dan
   d. staf yang tidak bersetuju atau melanggar syarat-syarat di dalam Dasar Am dan Dasar Khusus Emel.

5.4 Dasar Pembangunan Laman Web

i. Majlis menyediakan tapak untuk laman web rasmi Unit/Persatuan atau aktiviti rasmi sahaja.

ii. Ketua Unit/persatuan/organisasi adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan keselamatan laman web masing-masing. Pihak majlis tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan. Majlis boleh menghadkan atau memansuhkan akses kepada tapak laman web tersebut.

iii. Semua laman web Unit mesti mempunyai hubungan (link) dengan laman utama MUIP. Majlis berhak menukar atau mengubahsuai kandungan laman web atas kepentingan majlis.
iv. Majlis berhak menentukan perisian pembangunan laman web bagi tujuan pengoptimuman penggunaan dan keselamatan.
v. Laman web peribadi yang berbentuk ilmiah adalah dibenarkan tetapi perlu mendapat kelulusan Unit Teknologi Maklumat. Pihak majlis tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh Unit atau individu.
vi. Kandungan laman web mesti dipersembahkan dalam Bahasa Melayu dan Bahasa Inggeris. Penggunaan bahasa lain perlu mendapat kelulusan daripada majlis.
vii. Kandungan laman web hendaklah tidak mengandungi maklumat atau terdedah kepada kemasukan maklumat yang menyalahi undang-undang / peraturan majlis, negeri dan negara termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian.
viii. Semua laman web Unit/peribadi/persatuan yang dibangunkan sendiri perlu dimaklumkan kepada Unit Teknologi Maklumat dan mematuhi panduan yang ditetapkan.
ix. Fail-fail yang mempunyai extension .exe, .cmd, .bat, .mov, .avi, .mp3, .mpeg, .mpg, .wav, .rm, .ram, .rmx, .asf, .wmf, .wmp, dan .zip dan fail yang mempunyai kapasiti melebihi 1 *megabyte*. Fail-fail ini akan dibuang tanpa sebarang notis sekiranya dijumpai dalam tapak yang dihoskan.

5.5 Dasar Capaian Internet / Intranet

i. Majlis berhak menyedia dan memasang perisian penapisan isi kandungan Internet /Intranet.
ii. Laman-laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan. Laman yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan sama sekali, **kecuali** mendapat keizinan daripada Unit Teknologi Maklumat melalui sokongan ketua Jabatan bagi tujuan akademik, penyelidikan atau pentadbiran.
iii. Capaian laman yang berbentuk hiburan, hobi atau 'leisure' tidak dibenarkan di waktu pejabat, termasuk tetapi tidak terhad kepada laman ‘game online’, ‘radio online’ dan ‘video streaming’ yang membebankan rangkaian MUIP
iv. Melayari internet tanpa tujuan atau meninggalkan capaian Internet ‘unattended’ adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan rangkaian MUIP.
v. Majlis berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai.
vi. Pengguna dilarang mengganggu atau menceroboh laman Web mana-mana jabatan, organisasi atau negara.

vii. Pengguna dilarang memasuk, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang negara.

viii. 'Internet chatting' tidak dibenarkan. Penggunaan untuk tujuan rasmi perlu mendapat kelulusan daripada Unit Teknologi Maklumat secara bertulis melalui Ketua Jabatan. Permohonan hendaklah menyatakan tujuan penggunaan, senarai pengguna, dan perisian yang digunakan.

ix. 'Chatting' setempat untuk tujuan rasmi dibenarkan.

x. Pengguna tidak dibenarkan menggunakan sumber ICT MUIP untuk mendapat atau cuba mendapat capaian tidak sah (unauthorised) kepada mana-mana sistem komputer sama ada di dalam atau di luar MUIP. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem-sistem komputer tersebut atau mencapai sumber ICT MUIP dengan menggunakan identiti pengguna yang lain.

xi. Pengguna tidak dibenar mencapai atau cuba mencapai sumber elektronik (data, paparan, 'keystrokes', fail atau media storan) dalam sebarang bentuk yang dimiliki oleh pengguna yang lain tanpa mendapat kebenaran/kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian. Penggunaan penganalisis rangkaian (network analyzer) atau pengintip (sniffer) adalah dilarang.

xii. Pengguna yang mencapai sesuatu perkhidmatan yang perlu dibayar (contohnya pangkalan data 'online' komersial), hendaklah bertanggungjawab ke atas segala bayaran yang dikenakan.

BAB 6
DASAR AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT

6.1 Tujuan Dasar

Dasar ini menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di MUIP seperti berikut :

i. melindungi kepentingan pengguna utama ICT apabila berlaku kejadian pelanggaran atau pencabulan Dasar Keselamatan ICT;
ii. memelihara dan melindungi maklumat peribadi yang dimiliki MUIP;
iii. menyokong usaha MUIP untuk menjaga kepentingan "stakeholder";
iv. menerangkan aktiviti-aktiviti yang dilakukan oleh pentadbir operasi yang melibatkan capaian data, maklumat, atau kegiatan pengguna yang diklasifikasikan sebagai rahsia atau sulit.

6.2 Skop Dasar

Skop dasar ini meliputi tanggungjawab pengguna dan MUIP yang berkaitan capaian maklumat sulit.

Nota :*Bagaimanapun maklumat peribadi yang diambil untuk memudahkan seseorang individu berhubung, seperti alamat yang disediakan oleh seseorang individu adalah tidak termasuk dalam dasar ini.*

6.3 Dasar Capaian Maklumat Sulit

i. Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit.
ii. Pentadbir sistem berkuasa untuk mencapai, merekod, atau memantau data, maklumat atau kegiatan pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT. Maklumat-maklumat yang direkodkan ini akan digunakan untuk tujuan penjagaan keselamatan ICT. Contohnya, arahan dalam sistem komputer server UNIX seperti last, syslogd, acctcom, pacct yang berfungsi merekod aktiviti pengguna untuk tujuan pengauditan.
iii. Pentadbir sistem mempunyai kuasa tanpa mendapat kebenaran terlebih dahulu daripada pihak majlis untuk memantau kegiatan dan aktiviti pengguna yang melanggar Dasar Keselamatan ICT. Segala maklumat yang direkodkan boleh digunakan sebagai bukti. Sekiranya pelanggaran Dasar Keselamatan ICT tersebut serius seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, maka bukti-bukti yang dikumpul akan dimajukan kepada Jawatankuasa Keselamatan ICT MUIP.
iv. Pentadbir operasi boleh membuat salinan sama ada dalam bentuk bercetak atau digital kesemua atau sebahagian kandungan akaun pengguna sebagai pemeliharaan bukti. Pentadbir sistem dengan kebenaran majlis boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti emel atau fail-fail yang tersimpan dalam akaunnya.
v. Pengguna diberi jaminan bahawa selain daripada perkara-perkara yang disebutkan di atas, data, maklumat rahsia atau sulit yang terdapat dalam akaun pengguna tidak akan dicapai oleh sesiapa pun. Sekiranya ada individu atau pengguna lain mencapai data

atau maklumat pengguna lain tanpa kebenaran, maka individu tersebut (pengguna biasa atau pentadbir sistem) telah melanggar Dasar Capaian Teknologi Maklumat.

6.4 Dasar Pemantauan Data dalam Rangkaian

i. Pentadbir sistem berkuasa untuk memantau dan merekodkan data-data yang berada dalam rangkaian sebagai sebahagian daripada rutin penjagaan keselamatan sumber ICT. Peralatan rangkaian seperti *router* atau sistem komputer *server* yang menggunakan perisian-perisian tertentu mampu merekodkan data-data dalam rangkaian. Jaminan diberikan bahawa data-data yang direkodkan tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran Dasar Keselamatan ICT.

ii. Sama seperti kes capaian maklumat di atas sekiranya pentadbir operasi mengesyaki pengguna melanggar Dasar Keselamatan ICT, maka pentadbir operasi mempunyai mandat tanpa mendapat kebenaran majlis untuk memantau dan merekodkan data-data dalam talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data komunikasi sesi daripada mesin/peralatan yang digunakan oleh pengguna yang disyaki akan direkodkan, dan setiap 'keystroke' juga akan direkodkan. Data-data ini akan digunakan sebagai bahan bukti untuk proses pengauditan yang akan dilakukan oleh Jawatankuasa MUIP.

iii. Jaminan adalah diberikan kepada pengguna bahawa selain daripada perkara-perkara yang dinyatakan di atas, adalah menjadi kesalahan jika pengguna (pentadbir system atau pengguna biasa) memantau atau merekodkan data-data yang berada dalam rangkaian.

6.5 Dasar Pengurusan Maklumat Sulit/Peribadi

6.5.1 Pengambilan Maklumat Sulit / Peribadi

Pengurus yang menggunakan maklumat peribadi seseorang mestilah menyatakan tujuannya dengan jelas dan nyata seperti berikut :

(a.)apabila maklumat peribadi diambil daripada seseorang individu itu, maklumat itu mestilah diberikan oleh tuan punya maklumat tersebut dan bukan daripada orang lain; dan

(b.)pemberi maklumat hendaklah diberitahu / dimaklum untuk mengesahkan (tandatangan) sesuatu maklumat yang telah diberikan.

i. Kaedah Pengambilan Data

a. Maklumat peribadi diambil berpandukan dasar, peraturan atau undang-undang yang dibenarkan.
b. Maklumat peribadi tidak boleh diambil tanpa kebenaran atau tujuan yang jelas.
c. Maklumat peribadi yang terdapat di laman web atau portal MUIP adalah atas tanggungjawab penyedia laman web/portal tersebut. Majlis tidak bertanggungjawab ke atas kejituan maklumat peribadi yang disedia oleh Unit.

ii. Larangan Terhadap Pengambilan Maklumat Sensitif

Maklumat yang dinyatakan di bawah tidak boleh diambil, digunakan atau dihebahkan. Walau bagaimanapun jika maklumat diambil dengan mendapat kebenaran pemberi maklumat untuk mengambil, mengguna, menghebah ataupun untuk tujuan prosidur di dalam mahkamah, maka maklumat ini tidak termasuk di dalam Dasar ini iaitu :

- Bangsa
- asal keluarga
- agama, pandangan politik, ideologi atau pun keahlian sesuatu persatuan
- maklumat kesihatan, rawatan yang diambil

Nota :

- Semua maklumat yang sensitif hendaklah dinyatakan dengan jelas tujuan penggunaan data tersebut semasa permohonan mendapat maklumat dilakukan.

- Maklumat kesihatan hanya boleh diambil oleh Pegawai Perubatan yang bertauliah yang menguruskan pesakit-pesakit.

iii. Maklumat Sulit / Peribadi Yang Boleh Diambil Daripada Tuan Punya Maklumat

Maklumat peribadi berikut ataupun yang bersamaan dengannya boleh diambil :

- nama
- gelaran
- Unit
- nombor telefon
- alamat

Nota :

-Tujuan pengambilan dan penggunaan maklumat atau data hendaklah dimaklumkan kepada pemberi maklumat jika maklumat tersebut perlu dihebahkan untuk tujuan tertentu;

-Hak untuk meminta capaian kepada maklumat peribadi pemberi maklumat dan hak untuk mengubah apa-apa perubahan ataupun pembetulan jika terdapat kesalahan hendaklah dinyatakan.

iv. Had-Had Pengambilan Selain Daripada Pemberi Maklumat (Bukan Tuan Punya Maklumat)

Bagi kes di mana maklumat diambil daripada pihak ketiga, tuan punya maklumat hendaklah dimaklumkan tentang maklumat yang diambil dan tujuan penggunaan maklumat tersebut. Apabila maklumat yang diberi oleh seseorang kepada seseorang yang lain dengan izin pemberi maklumat, perkara berikut hendaklah diikuti :

- Tujuan pengambilan maklumat;
- Jenis maklumat yang diambil; dan
- Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

6.5.2 Had-Had Penggunaan

Maklumat peribadi mestilah digunakan untuk tujuan yang telah dinyatakan ketika
maklumat itu diperolehi daripada pemberi maklumat dalam skop yang dibenarkan oleh MUIP.

i. Had-had Penggunaan Untuk Tujuan Yang Diperlukan
   Penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat-syarat berikut :

   a. tuan punya maklumat telah memberi kebenaran menggunakan maklumat tersebut;
   b. maklumat boleh digunakan tuan punya maklumat bagi pengesahan sesuatu kontrak;
   c. maklumat boleh digunakan untuk tujuan mahkamah atau perundangan; dan
   d. maklumat boleh digunakan untuk melindungi tuan punya maklumat dalam semua perkara.

Nota :
Dalam menyediakan perlindungan yang efektif berkaitan maklumat peribadi seseorang, maklumat peribadi tidak boleh digunakan selain daripada syarat-syarat yang dijelaskan di atas.

ii. Penggunaan Maklumat Peribadi Untuk Tujuan Selain Daripada Yang Dinyatakan Ketika Maklumat Itu Diperolehi

   Apabila maklumat peribadi digunakan selain daripada tujuan asal ketika maklumat itu diambil, kebenaran daripada tuan punya maklumat mestilah diperolehi dengan kaedah yang dinyatakan dalam **Kaedah Pengambilan Data**. Tuan punya maklumat mempunyai hak untuk tidak memberi keizinan penggunaan maklumat tersebut.

6.5.3 Penyelenggaraan Maklumat Sulit / Peribadi

i. Majlis bertanggungjawab memastikan ketepatan maklumat peribadi semasa dalam simpanan dan sentiasa dikemaskini untuk tujuan yang diperlukan. Kemaskini maklumat hanya perlu dilakukan jika maklumat tersebut diperlukan oleh pihak MUIP. Dalam kes pemberi maklumat telah tamat perkhidmatan, beliau tidak dimestikan untuk mengemaskini maklumat tersebut kecuali apabila diperlukan oleh MUIP.
ii. Majlis bertanggungjawab menjamin keselamatan maklumat yang disimpan. Langkah-langkah keselamatan perlu diambil sama ada secara teknikal ataupun organisasi untuk mengelakkan maklumat dicapai secara tidak sah, dirosak, diubah, hilang dan sebagainya.
iii. Data dienkrip sekiranya disimpan dalam media elektronik untuk penghantaran secara rangkaian.
iv. Majlis bertanggungjawap menjamin kerahsiaan maklumat peribadi. Individu yang bertanggungjawab menyimpan, mengumpul atau

memproses data mestilah memastikan maklumat peribadi tidak disebarkan kepada pihak lain, selain daripada mereka yang mempunyai hak untuk mengetahui maklumat tersebut.

v. Permintaan untuk mencapai maklumat peribadi oleh tuan punya maklumat untuk tujuan pengesahan (verification) mestilah diberi untuk satu tempoh yang berpatutan. Jika terdapat kesilapan maklumat ketika diperiksa oleh tuan punya maklumat, penerima maklumat tersebut hendaklah diberitahu.

vi. Bantahan terhadap penggunaan maklumat peribadi oleh tuan punya maklumat hendaklah diterima. Walau bagaimanapun jika maklumat peribadi itu digunakan untuk tujuan pengesahan ataupun atas keperluan undang-undang MUIP, negeri atau negara, maka hak bantahan tersebut tidak dibenarkan.

vii. Pengurus maklumat mestilah memahami dan mengikuti Dasar ini, dan bertanggungjawab untuk memaklumkan kepada pemberi maklumat tentang Dasar ini.

BAB 7
DASAR KESELAMATAN ICT

7.1 Tujuan Dasar

Dasar ini bertujuan untuk :

i. memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer; dan
ii. menerangkan perlaksanaan keselamatan rangkaian MUIP yang merupakan satu infrastruktur rangkaian setempat (LAN) untuk penyambungan bagi tujuan komunikasi dan perkongsian maklumat/sumber.

7.2 Skop Dasar

Skop dasar merangkumi :

i. aspek keselamatan perkakasan, perisian sistem, pangkalan data dan sistem aplikasi; dan
ii. aspek rekabentuk keselamatan rangkaian.

7.3 Dasar Keselamatan Sistem Komputer/Server

7.3.1 Kawalan Capaian Fizikal

i. Kawalan terhadap individu/staf yang masuk ke Bilik Komputer dan juga kawalan akses kepada semua server serta sumber-sumber ICT lain; dan
ii. Mewujudkan mekanisma kawalan capaian fizikal untuk staf/individu mencapai server-server yang berkenaan.

7.3.2 Kawalan Capaian Logikal

Kawalan dibuat semasa instalasi agar hanya mereka yang dibenarkan sahaja boleh mencapai sistem. Mekanisma kawalan capaian adalah seperti berikut :

i. Identifikasi Pengguna

Pengguna sistem boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama. Dalam kedua-dua keadaan, pengguna perlu bertanggungjawab ke atas keselamatan sistem yang digunakan.

Langkah-langkah yang diambil untuk mengenalpasti pengguna yang sah ialah :

a) memberi satu ID yang unik kepada setiap pengguna individu;
b) menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti;
c) memastikan adanya kemudahan 'auditing' untuk menyemak semua aktiviti pengguna;
d) memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan dan tiada ID pengguna yang tidak diperlukan; dan
e) perubahan ID pengguna untuk sistem aplikasi perlu mendapat kebenaran daripada pemilik (owner) sistem tersebut.

Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan :

a) menggantung semua kemudahan (privilege) ID yang tidak digunakan selama 30 hari dan menghapus ID berkenaan selepas dari tempoh 30 hari tersebut; dan
b) menghapus semua kemudahan untuk pengguna yang berpindah atau tamat perkhidmatan.

'Audit trail' untuk setiap aktiviti pengguna hendaklah disimpan dan diarkib sekiranya keperluan storan adalah mencukupi terutamanya untuk pengguna yang boleh mencapai maklumat sulit agar dapat dikenalpasti sekiranya berlakunya pencerobohan maklumat.

ii. Autentikasi Pengguna

a) Proses bertujuan mengenalpasti hanya pengguna yang sah dibenarkan menggunakan sistem melalui penggunaan kata laluan. Sistem mestilah boleh menyediakan kemudahan bagi :

- kata laluan dimasukkan dalam bentuk yang tidak boleh dilihat ;
- panjang kata laluan sekurang-kurangnya 8 aksara;
- merupakan kombinasi daripada aksara,angka dan simbol-simbol lain;
- kata laluan dienkrip semasa penghantaran;
- fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan
- Cubaan capaian dihadkan kepada tiga (3) kali sahaja. ID pengguna berkenaan perlu digantung selepas tiga (3) kali cubaan gagal yang berturut.

7.3.3 Audit 'Trail'

Majlis bertanggungjawab menyedia dan menyimpan rekod 'audit trail' bagi mengenalpasti akauntabiliti pengguna dan keselamatan. Penggunaan 'audit trail' untuk sistem komputer dan manual operasi perlu diwujudkan untuk :

i. capaian kepada maklumat yang kritikal;
ii. capaian kepada perkhidmatan rangkaian; dan
iii. keistimewaan atau kebenaran tertentu yang melebihi kebenaran sebagai pengguna biasa digunakan seperti arahan-arahan keselamatan dan fungsifungsi 'superuser.'

Maklumat 'audit trail' merangkumi :

i. identifikasi (ID) pengguna;
ii. fungsi, sumber dan maklumat yang digunakan atau dikemaskini;
iii. tarikh dan masa penggunaan;
iv. alamat IP 'client' atau stesen kerja; dan
v. transaksi dan program yang dijalankan secara khusus.

Majlis akan mengambil tindakan berikut semasa penyediaan audit 'trail' :

i. meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera;
ii. meneliti 'audit trail' secara berjadual;

iii. meneliti dan melaporkan sebarang masalah keselamatan dan kejadian luar biasa;
iv. menyimpan maklumat 'audit trail' untuk jangka masa tertentu bagi keperluan operasi dan keselamatan; dan
v. mengawal maklumat 'audit trail' daripada dihapus, diubahsuai, ditipu atau disusun semula.

7.3.4 Penyalinan ('Backup') Maklumat

i. Majlis bertanggungjawab memulihkan sistem sepenuhnya jika berlaku masalah atau kerosakan.
ii. Proses penyalinan dibuat secara berjadual dan semasa perubahan konfigurasi pada sistem. 'Backup' perlu disimpan di tempat berasingan dan selamat.
iii. Majlis akan mengambil tindakan berikut semasa penyediaan penyalinan:
    a. mendokumen tatacara prosidur penyalinan dan pemulihan;
    b. menyimpan 3 generasi salinan; dan
    c. menguji media salinan dan tatacara prosidur pemulihan dua (2) kali setahun.

7.3.5 Penyelenggaraan

Majlis melaksana kawalan dan penyelenggaraan bagi memastikan integriti sistem pengoperasian daripada terdedah kepada sebarang pencerobohan keselamatan:

i. 'Patches' dan Kelemahan Sistem (Vulnerabilities)

Mengemaskini 'patches' dan mengatasi kelemahan sistem yang berlaku daripada agensi keselamatan berdaftar.

ii. Peningkatan (upgrades)

Menaiktaraf sistem pengoperasian kepada versi terkini.

7.4 Dasar Keselamatan Sistem Aplikasi

Majlis bertanggungjawab melaksana dan mengawal tahap capaian sistem aplikasi.

7.4.1 Perisian Aplikasi

Kawalan keselamatan dilaksana untuk mengelakkan berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. Majlis bertanggungjawab menyedia kawalan dan kemudahan seperti berikut:

i. sistem keselamatan berpusat dengan kawalan capaian penggunaan satu ID dan kata laluan untuk semua aplikasi;
ii. profil capaian yang menghad tahap capaian maklumat serta fungsi-fungsi berdasarkan peranan pengguna;
iii. kawalan peringkat sistem aplikasi yang menentukan akauntabiliti tertentu kepada pengguna; dan
iv. penetapan pemilik (ownership) maklumat.

7.4.2 Pangkalan Data

Majlis bertanggungjawap mengadakan kawalan capaian kepada pangkalan data.

Integriti maklumat yang disimpan di dalam pangkalan data dikekal dan dijamin secara :

i. sistem pengurusan pangkalan data memastikan integriti dalam pengemaskinian dan capaian maklumat; dan
ii. kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data.

7.4.3 Pengujian Aplikasi

Majlis bertanggungjawab menguji aturcara, modul, sistem aplikasi dan integrasi

sistem aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.

Majlis mengambil langkah berikut semasa pengujian aplikasi :

i. menggunakan data ujian (dummy) atau data lapuk (historical);
ii. mengawal penggunaan data terpilih(classified);
iii. menghadkan capaian kepada kakitangan yang terlibat sahaja;
iv. menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk); dan
v. menggunakan persekitaran yang berasingan untuk pembangunan dan pengoperasian sistem aplikasi.

7.4.4 Perisian Berkod Jahat (‘Malicious’) dan Rosak (Defective)

Aturcara sistem aplikasi terdedah kepada kod jahat dan kod rosak. Majlis bertanggungjawab mengurangkan kemungkinan perisian yang rosak melalui kawalan berikut :

i. mendapat kod sumber (source code) daripada pembangun sistem aplikasi yang bereputasi baik, rekod prestasi perkhidmatan yang baik dan mempunyai kepakaran teknikal yang tinggi;
ii. mewujud dan melaksana program jaminan kualiti dan prosidur untuk semua sistem aplikasi yang dibangunkan secara dalaman dan luaran; dan
iii. memastikan semua sistem aplikasi didokumen, diuji, disah fungsinya, tahan lasak(robustness) dan menepati spesifikasi.

7.4.5 Perubahan Versi (version)

Majlis bertanggungjawab mengawal versi sistem aplikasi apabila perubahan atau peningkatan dibuat dan mematuhi prosidur kawalan perubahan.

7.4.6 Penyimpanan Kod Sumber (Source Code)

Majlis bertanggungjawab mengurus dan melaksana kawalan penyimpanan kod sumber bagi sistem aplikasi yang dibangunkan secara dalaman atau luaran untuk tujuan penyelenggaraan dan peningkatan yang merangkumi:

i. mewujudkan prosidur penyelenggaraan versi terkini; dan
ii. mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada.

7.4.7 Perisian Tidak Berlesen

Majlis bertanggungjawab memastikan semua penggunaan perisian adalah berlesen serta mengawal dan menyimpan lesen serta kawalan fizikal ke atas lokasi perisian berlesen dan salinan lesen yang dikeluarkan.

7.4.8 Kawalan Kod Jahat (Malicious Code)

Majlis bertanggungjawab memastikan integriti maklumat daripada pendedahan atau kemusnahan akibat 'malicious code' seperti virus seperti berikut:

i. melaksanakan prosidur untuk mengurus kod jahat;
ii. mewujudkan peraturan berkaitan memuat turun, penerimaan dan penggunaan perisian percuma (freeware dan shareware);
iii. menyebarkan arahan dan maklumat untuk mengesan kod jahat kepada semua pengguna; dan
iv. mengambil langkah pencegahan atau pemulihan serangan kod jahat seperti berikut :
    - mengimbas dan menghapus kod jahat menggunakan perisian anti virus yang diluluskan majlis;
    - menyemak status proses imbasan dalam laporan log; dan
    - tidak melaksanakan (run) atau membuka fail kepilan (attachment) daripada e-mel yang meragukan.

7.5 Dasar Keselamatan Penggunaan Emel

7.5.1 Akaun Emel

i. Akaun emel bukan hak mutlak seseorang tetapi kemudahan yang disediakan tertakluk kepada peraturan Majlis dan boleh ditarik balik jika melanggar Dasar Internet/Intranet.

7.5.2 Menyenggara Kotak Mel (Mail Box)

i. Kandungan dan penyelenggaraan kotak mel pada komputer peribadi adalah menjadi tanggungjawab pengguna.
ii. Pengguna hendaklah sentiasa mengimbas fail dalam kotak mel dengan perisian anti-virus bagi memastikan fail yang dihantar/diterima melalui lampiran (attachment) bebas daripada virus.
iii. Emel hendaklah tidak mengandungi maklumat rahsia atau sulit yang boleh disalah guna untuk merosakkan akaun, stesen kerja, komputer server dan rangkaian MUIP.

7.5.3 Penggunaan Perisian Mel

i. Pengguna hendaklah mengguna perisian mel rasmi MUIP yang lebih selamat daripada ancaman dan penyebaran kod jahat berbanding perisian lain seperti Microsoft Outlook, IncrediMail dan lain-lain.

ii. Pengguna yang tidak menggunakan perisian mel rasmi MUIP hendaklah sentiasa membuat penyalinan terhadap data-data emel.

7.6 Dasar Keselamatan Peralatan Rangkaian

7.6.1 Keselamatan Fizikal

i. Peralatan rangkaian hendaklah ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, kilat, gegaran, kekotoran dan sebagainya.
ii. Suhu hendaklah terkawal di dalam had suhu peralatan rangkaian berkenaan dengan memasang sistem penghawa dingin sepanjang masa.
iii. Memasang Uninterruptible Power Supply (UPS) dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik dan perlindungan daripada kilat dan menyokong penutupan (shut down) server secara automatik.

7.6.2 Capaian Fizikal

a) Capaian Pengkabelan Rangkaian

Langkah-langkah yang perlu diambil untuk melindungi kabel rangkaian daripada dicapai oleh orang yang tidak berkenaan :

i. melindungi pengkabelan di dalam kawasan awam dengan cara memasang 'conduit' atau lain-lain mekanisma perlindungan; dan
ii. pusat pendawaian terletak di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

b) Capaian Peralatan Rangkaian

i. Peralatan hendaklah ditempatkan di tempat yang selamat dan terkawal.
ii. Peralatan rangkaian hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

7.6.3 Capaian Logikal

i. ID dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh kakitangan yang dibenarkan sahaja.
ii. Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan.
iii. Maklumat capaian ke *router* hendaklah direkodkan - pegawai, tarikh, masa dan aktiviti. Maklumat mestilah disimpan selama 90 hari.
iv. Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja. Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan termasuk pengguna yang membuat perubahan, pengesahan, tarikh dan masa.Perubahan perisian konfigurasi mestilah direkodkan – pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.
v. Perubahan konfigurasi hendaklah dikendalikan secara berpusat.

7.6.4 Penggunaan Peralatan Tanpa Kebenaran

i. Mengadakan kawalan capaian logikal seperti yang disebutkan di para 7.6.3.
ii. Menempatkan peralatan di tempat yang selamat dan terkawal.
iii. Bilik pendawaian atau 'wiring closet' hanya boleh dicapai oleh pegawai yang dibenarkan sahaja.
iv. Menyelenggara inventori peralatan dan membuat semakan secara berkala.

7.6.5 Konfigurasi Peralatan

i. Mengaktifkan (enable) perkhidmatan yang diperlukan sahaja.
ii. Menghadkan capaian konfigurasi kepada nod atau alamat IP yang dibenarkan sahaja.
iii. Mematikan (disable) penyiaran trafik (broadcast).
iv. Menggunakan kata laluan yang selamat.
v. Dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.

7.6.6 Penyelenggaraan Peralatan

i. Peralatan hendaklah dipasang, dioperasi dan diselenggarakan mengikut spesifikasi pengilang.
ii. Dibaiki dan diselenggara hanya oleh kakitangan yang terlatih dan dibenarkan sahaja.
iii. Mengemaskini rekod penyelenggaraan.

7.7 Dasar Kebolehcapaian Pengguna (User Accessibility)

7.7.1 Rangkaian Setempat (Local Area Network)

i. Hanya staf MUIP dibenarkan membuat penyambungan ke rangkaian MUIP (rujuk Dasar Rangkaian).
ii. Pengguna luar perlu mendapatkan kebenaran daripada Ketua Unit Teknologi Maklumat sebelum membuat capaian ke rangkaian MUIP.
iii. Hanya pengguna yang disahkan sahaja dibenarkan membuat capaian kepada sistem pengkomputeran MUIP.
iv. Perisian pengintip (sniffer) atau penganalisis rangkaian (network analyzer) tidak dibenar digunakan pada sebarang komputer kecuali setelah mendapat kebenaran daripada Majlis. Status komputer hendaklah disemak setiap tahun.

7.8 Dasar Sambungan Dengan Lain-Lain Rangkaian

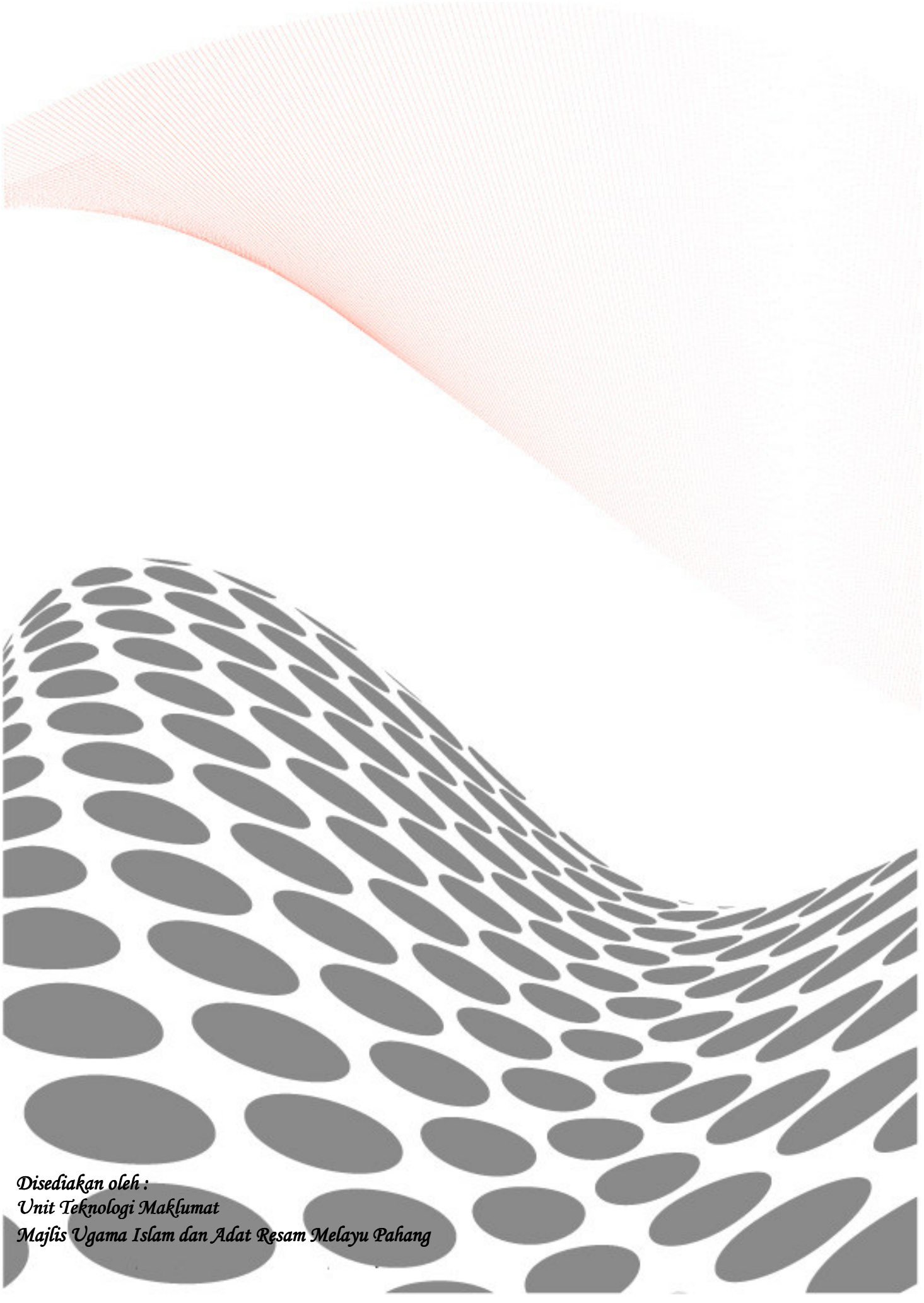
7.8.1 Capaian Yang Tidak Digalakkan

i. Penggunaan protokol rangkaian seperti NetBIOS dan IPX/SPX.
ii. Penggunaan workgroup kerana menyokong 'share-level security'.

7.8.2 'Firewall'

i. Semua trafik rangkaian daripada dalam ke luar MUIP dan sebaliknya mestilah melalui 'firewall' dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan kepada Dasar Rangkaian.
ii. Rekabentuk 'firewall' hendaklah mengambilkira perkara-perkara berikut :
    - keperluan audit dan arkib;

- kebolehsediaan;
- kerahsiaan; dan
- melindungi maklumat/majlis.



Disediakan oleh :
Unit Teknologi Maklumat
Majlis Ugama Islam dan Adat Resam Melayu Pahang