POLISI DAN PERATURAN KESELAMATAN ICT

LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR

DISEMBER 2022

Versi 3.0

ISI KANDUNGAN	M/S
BAB 1- DASAR UMUM TEKNOLOGI MAKLUMAT	1- 12
PENGENALAN	1
OBJEKTIF	1-2
PENYATAAN DASAR	3-4
SKOP	5-7
PENILAIAN RISIKO KESELAMATAN ICT	8
1.1 SKOP DASAR	9
1.2 DAFTAR KATA	9
1.3 DASAR UMUM ICT LPHS	10
1.4 DASAR TEKNOLOGI MAKLUMAT	11
1.5 PELANGGARAN DASAR	12
BAB 2- DASAR KHUSUS TEKNOLOGI MAKLUMAT	13-50
2.1 PENGURUSAN ICT	13-16
2.2 PERISIAN, APLIKASI DAN PERKAKASAN ICT	16-21
2.3 RANGKAIAN ICT	22-26
2.4 KEMUDAHAN ICT	26-35
2.5 AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT	35-37
2.6 KESELAMATAN ICT	37-43
SURAT AKUAN PEMATUHAN	44
SENARAI PERUNDANGAN DAN PERATURAN	45

PENGENALAN

Lembaga Perumahan Dan Hartanah Selangor berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integritI dan teknologi. Dokumen ini menerangkan polisi penggunaan sumber-sumber Teknologi Maklumat (ICT) yang diterima pakai sebagai Dasar Umum ICT Lembaga Perumahan Dan Hartanah Selangor (LPHS) dan peranan mereka melindungi aset ICT Lembaga Perumahan Dan Hartanah Selangor. Dokumen ini diguna pakai oleh semua pihak kakitangan, pengguna dan pembekal yang menyediakan perhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di Lembaga Perumahan Dan Hartanah Selangor. Mana-mana dasar khusus dan terperinci untuk setiap sumber yang disenarai adalah mengatasi Dasar Umum ini.

OBJEKTIF

Dasar Keselamatan ICT (DKICT) Lembaga Perumahan Dan Hartanah Selangor diwujudkan untuk menjamin kesinambungan urusan Lembaga Perumahan Dan Hartanah Selangor (LPHS) dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga sesuai untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi LPHS. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama DKICT di LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR adalah seperti berikut: -

1. Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;

2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan maklumat dan komunikasi;

3. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

4. Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;

5. Memperkemaskan pengurusan risiko;

6. Mencegah penyalahgunaan atau kecurian aset ICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR; dan

7. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

Penggunaan sumber ICT oleh kakitangan LPHS merupakan *instrument* asas yang penting untuk mencapai Visi dan Misi LPHS. Oleh itu dasar ini diperlukan bagi tujuan untuk memastikan:

i. Warga LPHS dimaklumkan mengenai kewujudan dan peranan UTM dalam melaksana dan menguatkuasakan dasar-dasar ICT LPHS;

ii. Kemudahan ICT digunakan secara bijaksana mengikut dasar yang ditetapkan;

iii. Tanggungjawab pengguna dimaklumkan secara jelas.

PENYATAAN DASAR

Keselamatan ditakrif 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 dimana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR 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 hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Citi-ciri utama keselamatan maklumat adalah seperti berikut:

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

5. **Ketersediaan** – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah kea rah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa tahap 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.

SKOP

Aset ICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data. DKICT LEMBAGA PERUMAHAN DAN HARTNAH SELANGOR telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

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

2. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatanya sepanjang masa, DKICT LEMBAGA PERUMAHAN DAN HATANAH SELANGOR ini merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Perkakasan

   Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR. Contoh peratan dan peripheral seperti computer, pelayan, *firewall,* pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *uninterruptible Power Supplu (*UPS) dan sebagainya;

2. Perisian

   Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian computer yang disimpan di dlaam sistem ICT. Contoh aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR.

3. Perkhidmatan

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

   i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

   ii. Sistem halangan akses seperti sistem kad akses; dan

   iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain.

4. Data dan maklumat

   Koleksi fakta-fakta dalam bentuk kerjata atau mesej elektronik, yang mengangungi maklumat-maklumat yantk digunkaan bagi mencapai misi dan objektif LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR. Contohnya sistem dokumentasi, prosedur operasi, rekod-rekod LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR, profil-profil pelanggan, pangkalan data dan fail-fail data, malumat-maklumat arkib dan lain-lain;

5. Manusia

   Semua pengguna infrastruktur ICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR bagi mencapai misi dan objektif jabatan. Indicidu berkenaan merupakan aset berdasekan kepada tugas-tugas dan fungsi yang dilaksanakan.

6. Media storan

   Semua media storan dan peralatan yang berkaitan seperti diske, storan mudah aliah, kartrij, CD-ROM, pita, cakera, pemacu cakera, pemacu pita dan lain-lain;

7. Media komunikasi

   Semua peralatan berkaitan komunikasi seperti pelayan rangkaian, gateway, bridge, router, peralatan PABX, wireless LAN, talian ISDN, peralatan video conferencing, modem, PCMCIA, kabel rangkaian, NIC, switches, hub dan lain-lain;

8. Dokumentasi

   Semua dokumen (prosedur dan manual pengguna) yang berkaitan dengan aset ICT, pemasangan dan pengoperasian peralatan dan perisian, sama ada dalam bentuk elektronik atau bukan elektronik.

9. Premis Komputer dan Komunikasi

   Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 8 di atas. Setiap perkara di atas perlu diberi perlindungan rapi, sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelangggaran langkah-langkah keselamatan.

PENILAIAN RISIKO KESELAMATAN ICT

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

LEMBAGA PERUMAHANDANHARTANAH SELANGOR hendaklah melaksanakan penilaian risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya megambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau megawal risiko keselamatan ICT berdasarkan penemuan penialaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di permis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utility dan sistem-sistem sokongan yang lain.

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

LEMBAGA PERUMAHANDANHARTANAH SELANGOR perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko yang berlaku dan memilih tindakan berikut:-

a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

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

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

d. Memindahkan risiko ke pihak laian seperti pembekal, pakar perunding dan pihak-pihak lain yang berkepentingan.

1.1 Skop Dasar

i. Sumber

Sumber-sumber yang tersenarai di dalam dokumen, juga sumber-sumber yang tidak tersenarai tetapi dianggap sebagai sumber ICT oleh Jawatankuasa ICT (JKICT) adalah tertatkluk kepada dasar ini.

ii. Pengguna

Semua pengguna adalah tertakluk kepada dasar ini. Sesiapa yang tidak diberi kebenaran adalah dianggap melakukan kesalahan, dan boleh diambil tindakan yang bersesuaian dengan kesalahan yang dilakukan.

1.2 Daftar kata

LPHS	Lembaga Perumahan Dan Hartanah Selangor
UTM	Unit Teknologi Maklumat
ICT	Teknologi Maklumat
PPTM	Penolong Pegawai Teknologi Maklumat
Kakitangan	Kakitangan Lembaga Perumahan Dan Hartanah Selangor
Pengguna	Kakitangan dan/ atau orang yang diberi kebenaran menggunakan sistem di LPHS
BTM	Bahagian Teknologi Maklumat Negeri
DKICT Negeri	Dasar Keselamatan ICT Negeri

1.3 Dasar Umum ICT LPHS

i. LPHS hendaklah menyediakan kemudahan ICT bagi kegunaan kaitangan bagi menyokong fungsi LPHS.

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

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

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

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

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

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

viii. Dasar ini adalah tertakluk kepada perubahan dari semasa ke semasa.

1.4 Dasar Teknologi Maklumat Peringkat Kebangsaan

Dasar Am ini adalah tertakluk kepada kandungan dokumen ini, malah ia turut mencakupi serta menerima pakai dasar-dasar ICT peringkat kebangsaan seperti berikut:

Dasar Keselamatan ICT Kerajaan berdasarkan Pekeliling Am Bil. 3 Tahun 2000 yang dikeluarkan oleh MAMPU (Lampiran 1);

Garis Panduan Malaysia Civil Service Link (MCSL) dan Laman Web Kerajaan berdasarkan Pekeliling Am Bil. 1 Tahun 2000 yang dikeluarkan oleh MAMPU (Lampiran 2);

Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat berdasarkan Pekeliling Am Bil. 6 Tahun 1999 yang dikeluarkan oleh MAMPU (Lampiran 3);

Penubuhan Jawatankuasa IT dan Internet Kerajaan (JITIK) berdasarkan Pekeliling Am Bil. 2 Tahun 1999 yang dikeluarkan oleh MAMPU (Lampiran 4);

Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) melalui Pekeliling Am Bil. 1 Tahun 2001 yang dikeluarkan oleh MAMPU (Lampiran 5); dan

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

a) Tandatangan Digital 1997 (Lampiran 6)
b) Hakcipta (amendment) 1997 (Lampiran 7)
c) Jenayah Komputer 1997 (Lampiran 8)
d) Tele-medicine 1997 (Lampiran 9)
e) Komunikasi dan Multimedia 1998 (Lampiran 10)
f) Suruhanjaya komunikasi dan Multimedia Malaysia 1998 (Lampiran 11)

Dasar-dasar ICT ini sah sehingga terdapat pindaan

1.5 Pelanggaran Dasar

i. Sebarang pelanggaran dasar dan peraturan oleh pengguna akan dikenakan tindakan.

ii. Sebarang aduan tentang pelanggaran Dasar hendaklah dibuat secara bertulis kepada Jawatan kuasa ICT, Jawatankuasa 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 ICT adalah penggantungan penggunaan kemudahan ICT dan lain-lain tindakan yang dirasakan perlu.

iv. Sebarang pelanggaran dasar dan peraturan berunsurkan jenayah akan dirujuk kepada Jawatankuasa Tatatertib yang berkaitan dengan mengikut prosedur yang ditetapkan.

BAB2- DASAR KHUSUS TEKNOLOGI MAKLUMAT

2.1 Pengurusan ICT

A. Tujuan Dasar

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

B. Skop Dasar

Skop Dasar melibatkan:

a. aspek pengurusan organisasi ICT yang mempunyai kuasa dan kepakaran untuk merancang, melaksana dan mengurus keperluan ICT LPHS menerusi strategi-strategi yang ditetapkan; dan

b. aspek pembangunan ICT bagi merancang, mengurus, melaksana dan menyelenggara keperluan ICT LPHS menerusi strategi-strategi yang ditetapkan.

C. Pengurusan Organisasi

a. Penubuhan Jawatankuasa ICT

i. Menubuhkan jawatankuasa untuk menggubal dasar, arah tuju dan matlamat ICT LPHS
ii. Melulus perancangan projek ICT LPHS
iii. Pengerusi Jawatankuasa ialah Ketua Penolong Pengarah.
iv. Jawatankuasa dianggotai oleh semua Ketua Unit
v. Unit Teknologi Maklumat (UTM) ialah seketariat bagi jawatankuasa ini.

b. Penubuhan Unit Teknologi Maklumat (UTM)

i. UTM bertanggungjawab dalam merancang, melaksana, mengurus, memantau dan menyelenggara projek-projek ICT LPHS.

ii. UTM diketuai oleh seorang Penolong Pegawai Teknologi Maklumat (PPTM)

iii. UTM perlu mempunyai kakitangan yang mempunyai keparan ICT yang secukupnya

iv. UTM akan mengendalikan Mesyuarat Pengurusan/ Teknikal ICT dari semasa ke semasa yang dipengerusikan oleh Ketua Penolong Pengarah.

D. Pembangunan ICT

a. Perancangan ICT

i. Perancangan hendaklah memenuhi fungsi dan keperluan LPHS dalam pengajaran, pembelajaran, penyelidikan, perundingan, pentadbiran dan pengurusan LPHS

ii. Perancangan hendaklah selaras dengan agenda ICT Negara

iii. Perancangan hendaklah mematuhi Dasar, Peraturan dan Garis Panduan yang ditetntukan oleh pihak Kerajaan Malaysia.

b. Perolehan ICT

i. Semua perolehan hendaklah mematuhi Dasar Perolehan serta Kewangan LPHS dan Kerajaan.

ii. Perolehan hendaklah memenuhi teknologi terkini dengan mendapat perakuan spesifikasi oleh Jawatankuasa Teknikal UTM

iii. Semua perisisan aplikasi dan perisian sistem hendaklah mempunyai lesen yang sah

iv. Semua pembangunan atau perolehan sistem aplikasi hendaklah dibuat melalui Jawatankuasa Teknikal UTM bagi menjamin keseragaman, keserasian dan keselamatan sistem

c. Instalasi dan Penyelenggaraan

i. Semua instalasi atau pemasangan perkakasan dan/ atau perisian dilakukan di bawah penyeliaan UTM

ii. Ketua Unit hendaklah bertanggungjawab memastikan peralatan ICT disenggara sewajarnya berdasarkan khidmat nasihat Penolong Pegawai Teknologi Maklumat (PPTM)

d. Naiktaraf atau pelupusan

i. Semua naik taraf perkakasan dan perisian hendaklah mendapat kelulusan Jawatankuasa Teknikal UTM

ii. Perkakasan yang tidak berkeupayaan dan/atau tidak sesuai untuk dinaiktaraf atau diperbaiki boleh dicadang untuk pelupusan mengikut Prosedur Pelulusan Kerajaan.

e. Pembangungan sumber manusia

i. Merancang keperluan sumber manusia yang secukupnya bagi menyokong perkhidmatan ICT LPHS

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 LPHS

f. Keselamatan ICT

Semua pengguna hendaklah mematuhi :

i. Dasar Penggunaan Bahan dan Perkakasan ICT;

ii. Dasar Keselamatan ICT LPHS;

iii. Dasar Keselamatan ICT Kerajaan (Pekeliling Am Bil. 3 Tahun 2000); dan

iv. Akta/ undang –undang berkenaan yang digubal oleh Kerajaan Malaysia.

2.2 Perisian, Aplikasi dan Perkakasan ICT

A. Tujuan Dasar

Menentukan tanggungjawab pengguna dan pihak LPHS mengenai perkara-perkara yang berhubung dengan perisian, aplikasi dan perkakasan ICT LPHS

B. Skop Dasar

Melibatkan semua perisian, aplikasi dan perkakasan LPHS yang dimiliki, diguna, dibangun, diperolehi atau berada di dalam simpanan pengguna ICT LPHS.

C. Perisisan dan Aplikasi

a. Haklimilik

i. Semua perisian dan aplikasi yang diperolehi untuk atau bagi pihak LPHS atau semua perisian yang dibangunkan oleh kakitangan atau vendor untuk tujuan pengurusan dan pentadbiran adalah menjadi hak LPHS.

ii. Bagi perisian dan aplikasi yang dibangunkan, maklumat tentang semua pengara/ pencipta mestilah dikekalkan.

iii. Semua perisian dan aplikasi hakmilik LPHS tidak dibernarkan dijual, disewa, dilesenkan semula, dipinjam, disalian semula, disebara atau diberi kepada sesiapa atau entiti tanpa kebenaran LPHS.

b. Perolehan Perisian dan Aplikasi

i. Semua perolehan perisian dan aplikasi hendaklah mengikut prosedur perolehan LPHS.

ii. Semua perolehan perisian untuk kegunaan LPHS hendaklah menggunakan versi terkini dan pelesenan akademik seperti *academic edition* (AE), *academic license* atau *education edition*.

iii. Penggunaan adalah tertakluk kepada terma dan syarat penggunaan yang ditetapkan oleh pihak LPHS, pembekal atau pembangunan perisian.

iv. LPHS tidak akan bertanggunjawab terhadap sebarang perolehan dan penggunaan perisian tanpa lesen yang dilakukan oleh pengguna.

v. LPHS bertanggungjawab melaksanakan peningkatan dan naiktaraf perisian dan aplikasi bagi memastikan versi yang sesuai digunapakai.

vi. LPHS bertanggungjawab menyediakan perkhidmatan penyenggaraan bagi aplikasi yang memerlukan kepakaaran khusus mengikut tempoh yang sesuai.

vii. LPHS menggalakkan penggunaan dan pembangunan aplikasi dan perisian sumber terbuka.

c. Tanggungjawab pengguna

i. Semua pengguna secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan pelesenan bagi setiap perisian yang digunakan.

ii. Semua pengguna tidak dibenarkan memuat turun, membuat instalasi dan mengguna perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian intranet LPHS misalnya

perisian P2P (peer to peer) internet seperti Kazaa, Imesh, Morpheus, Grokster dan sebagainya kecuali di UTM.

iii. Semua pengguna tidak dibenarkan menyebar sebarang perisisan berlesen secara tidak sah. LPHS tidak akan bertangggungjawab ke atas sebarang kesalahan yang dilakukan oleh pengguna.

iv. Sebarang bentuk permainan komputer tidak dibenarkan kecuali untuk tujuan akademik dan penyelidikan setelah mendapat kelulusan daripada Ketua Pengarah Eksekutif.

v. Sebarang kerosakan aplikasi hendaklah dilaporkan kepada UTM melalui Ketua Unit kecuali sebarang aplikasi yang diperolehi khas oleh unit dimana ia menjadi tanggungjawab unit berkaitan untuk melaporkan kepada pihak berkenaan (pembekal dan sebagainya).

D. Perkakasan

a. Hakmilik

i. Semua perkakasan yang diperolehi untuk atau bagi pihak LPHS atau semua perkakasan yang dicipta atau dipasang mengguna peruntukan LPHS oleh kakitangan LPHS adalah menjadi hakmilik LPHS.

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 entity tanpa kebenaran LPHS.

b. Perolehan Perkakasan

i. Semua perolehan perkakasan hendaklah mengikut prosedur perolehan LPHS.

ii. Spesifikasi perkakasan hendaklah diperakukan oleh Jawatankuasa Teknikal LPHS bagi memastikan piawaian dan keseragaman dari segi teknikal dan keperluan semasa.

iii. Setiap perolehan perkakasan hendaklah dimaklumkan kepada UTM untuk pengesahan spesifikasi perolehan dan tujuan rekod dan inventori LPHS.

c. Pengagihan Perkakasan

i. Semua pengagihan perkakasan hendaklah mengikut prosedur LPHS.

ii. Setiap pengguna yang layak menerima komputer hanya layak mendapat peruntukan satu unit komputer dalam satu-satu masa.

iii. Kakitangan kategori lain – layak diberi komputer bedasarkan keperluan kerja yang ditentukan oleh Ketua Unit. Sebarang permohonan individu atau berkumpulan hendaklah dibuat secara bertulis kepada UTM dengan mendapat perakuan Ketua Unit.

iv. Kakitangan yang tamat perkhidmatan atau yang melanjut pengajian, perlu memaklumkan kepada ketua unit dan memulangkan perkakasan di bawah tanggungjawabnya kepada UTM.

d. Peminjaman Perkakasan

i. Semua peminjam perkakasan hendaklah mengikut prosedur atau terma yang telah diterima pakai oleh pihak LPHS.

ii. Setiap unit yang menyediakan peminjaman perkakasan perlu merekodkan maklumat berkaitan peminjaman dan pemulangan.

iii. Peminjam bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam.

iv. Peminjam perlu memulangkan perkakasan yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan.

v. Peminjam perlu mengganti atau membayar kos perkakasan sekiranya berlaku kerosakan atau kehilangan perkakasan yang dipinjam.

vi. Tempoh pinjaman adalah tertakluk kepada kelulusan UTM.

e. Baik Pulih dan Penyelenggaraan Perkakasan

i. Semua baik pulih dan penyenggaraan perkakasan hendaklah mengikut prosedur LPHS.

ii. Bagi kerosakan perkakasan yang dibekalkan oleh UTM, ketua unit dikehendaki membuat aduan kepada UTM melalai saluran aduan yang disediakan secara borang berkaitan atau telefon, urusan pembaikan dan penyenggaraan akan diuruskan sepenuhnya oleh UTM.

iii. Bagi kerosakan perkakasan yang dibeli menggunakan bajet unit, unit diminta membuat aduan kepada UTM untuk tujuan pemeriksaan dan pengesahan kerosakan dam unit perlu menghubungi pembekal perkakasan tersebut untuk dibaiki.

iv. LPHS bertanggungjawab meyediakan perkhidmatan penyenggaraan bagi perkakasan yang memerlukan kepadakaran khususs mengikut tempoh yang sesuai.

f. Pelupusan Perkakasan

i. Semua perkakasan yang didapati tidak sesuai dinaik taraf atau disenggara hendaklah dilupus mengikut prosedur Pelupusan LPHS.

ii. Bagi perkakasan yang dibekalkan oleh UTM, UTM akan membuat cadangan pelupusan kepada Jawatankuasa Pelupusan LPHS.

iii. Bagi perkakasan yang dibeli menggunakan bajet unit, unit diminta membuat laporan cadangan kepada Jawatankuasa Teknikal ICT yang dipengerusikan oleh Ketua Penolong Pengarah untuk semakan dan pengesahan bagi tujuan pelupusan kepada jawatankuasa Pelupusan LPHS.

iv. Mana-mana perkakasan yang dilupuskan akan diganti baru oleh UTM.

g. Sewa Perkakasan

i. Semua perkakasan yang hendak disewa mestilah melalaui UTM

ii. Bagi perkakasan di bawah tanggungjawab unit hendaklah disewa melalui unit

iii. Semua perkakasan yang disewa adalah tertakluk kepada perjanjian yang diterima pakai oleh Pengurusan LPHS.

h. Tanggungjawab pengguna

i. Pengguna tidak berhak mengganggu dengan apa cara sekalipun perkakasan yang bukan berada di 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 perkongsian perlu mempunyai syarat dan peraturan yang dipersetujui oleh pengguna.

iii. Melapor segera secara bertulis kepada UTM melalui dan dengan perakuan ketua unit sekiranya perkakasan tersebut rosak atau tidak berfungsi untuk tujuan pembaikan atau gantian.

iv. Melaporkan segera secara bertulis kepada UTM sekiranya perkakasan tersebut hilang atau dicuri dan membuat laporan berdasarkan Peraturan Kewangan Dan Perakuan Berkenaan Kehilangan Wang atau Harta LPHS bagi peralatan yang dibekalkan oleh UTM

2.3 Rangkaian ICT

A. Tujuan Dasar

Dasar ini menentukan penyediaan, penggunaan dan pengoperasian komputer server, perkhidmatan Rangkaian Intranet LPHS dan penyambungan infrastruktur rangkaian.

B. Skop Dasar

Skop dasar adalah merangkumi:

a. 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).

b. Perkhidmatan Rangkaian Intranet LPHS – Merangkumi semua sumber rangkaian, termasuk peralatan rangkaian seperti *switches* dan *router*, perisian aplikasi rangkaian seperti *e-mail, web browser* dan *ftp*, konsep konfigurasi rangkaian seperti penggunaan alamat IP dan teknologi dan protocol rangkaian yang diguna seperti teknologi Gigabit dan protocol TCP/IP. Aktiviti ini juga perlu merukuk kepada DKCIT Negeri selaku orang atau entiti yang menyediakan rangkaian Internet dan Intranet.

C. Piawaian Prosedur Operasi

a. Semua pengguna komputer di dalam makmal (sama ada yang disambung ke Intranet LPHS atau tidak) mesti direkodkan ke dalam buku log atau sistem yang dikuatkuasa. Rekod tersebut hendaklah mempunyai sekurang-kurangnya meklumat berikut:

i. Tarikh
ii. Nama pengguna
iii. Nombor kad pengenalan
iv. Masa mula penggunaan
v. Masa tamat penggunaan
vi. Tandatangan pengguna

b. Buku log atau sistem ini (sama ada berbentuk digital atau manual) perlu disimpan dengan baik sekurang-kurangnya untuk tempoh dua (2) tahun bagi tujuan rujukan jika diperlukan.

D. Komputer server

a. Hakmilik

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

b. Perolehan

i. Semua perolehan hendaklah mengikut prosedur perolehan LPHS.

ii. Spesifikasi komputer server hendaklah diperakukan oleh Jawatankuasa Teknikal UTM bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa.

iii. Setiap perolehan komputer server hendaklah dimaklumkan kepada UTM untuk pengesahan spesifikasi perolehan dan tujuan rekod serta aset LPHS.

c. Konfigurasi dan Operasi

i. Semua komputer server untuk kegunaan dalaman akan diberi alamat IP static.

ii. Semua komputer server perlu didaftarkan dengan UTM, berada di dalam domain LPHS dan perlu dinyatakan dengan jelas fungsi tersebut.

iii. Pentadbir sistem perlu memastikan keselamatan server daripada pencerobohan termasuk pemeriksaan ke atas proses tersembunyi (*hidden prosesss*), '*daemons*', mengemaskini perisisan seperti email dan laman web serta mengenalpasti tahap capaian pengguna dan penggunaan komputer server.

iv. Komputer server yang digunakan untuk tujuan penyelidikan yang menggunakan rangkaian secara intensif (*high bandwidth usage*) perlu ditempatkan dalam rangkaian persendirian yang dipisahkan daripada Intranet LPHS melalui penggunaan '*switch*' untuk mengelak gangguan kepada rangkaian utama. Sebarang ujian yang memerlukan penggunaan rangkaian Intranet LPHS secara terus perlu mendapat kelulusan daripada

Setiausaha Bahagian, Bahagian Teknologi Maklumat SUK, Selangor melalui UTM.

v. Komputer server untuk kegunaan lain (contoh kafe siber) tidak dibenarkan menggunakan rangkaian Intranet LPHS untuk mengelak ganggunan rangkaian.

vi. Alamat IP tidak dibenarkan diubah sama sekali kecuali setelah mendapat kelulusan UTM

vii. Login dan kata laluan untuk id '*root*' dan '*super user*' adalah di bawah kawalan dan tanggungjawab pentadbir komputer server sepenuhnya.

E. Rangkaian Intranet LPHS

a. Hakmilik

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

b. Perolehan

i. Semua perolehan sumber rangkaian hendaklah mengikut prosedur perolehan LPHS.

ii. Perolehan peralatan rangkaian seperti *switch* dan *wireless access point* oleh LPHS adalah tidak dibenarkan kecuali dengan kelulusan Jawatankuasa
Teknikal LPHS.

c. Kemudahan Rangkaian Intranet LPHS

i. Pengguna tidak dibenarkan dalam apa bentuk sekali pun mengganggu lain-lain pengguna Intranet LPHS, Internet dan sebarang rangkaian yang lain termasuk menghantar maklumat rambang email atau mesej atas talian (*on-line*).

ii. Pengguna tidak boleh memberi sumber rangkaian di bawah jagaanya termasuk diagram nod rangkaian dan kad rangkaian tanpa wayar untuk

diguna oleh orang lain walaupun kepada kakitangan LPHS tanpa mendapat kelulusan pentadbir rangkaian.

iii. Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti yang dilakukannya kepada stesen kerja, komputer peribadi atau PDA yang melibatkan atau melalui Intranet LPHS termasuk akses ke Internet dan rangkaian-rangkaian yang lain.

iv. Mana-mana komputer yang menjadi sumber ancaman atau penyebaran virus akan disekat capaiannya ke Intranet LPHS. Perkhidmatan Intranet LPHS akan ditutup sehingga komputer tersebut disahkan bebas dari ancaman virus.

d. Penyambungan Rangkaian.

i. Kelulusan dari UTM perlu diperolehi untuk sebarang pembelian peralatan rangkaian dan penyambungan ke Intranet LPHS perlu mendapat kelulusan daripada UTM. Konfigurasi penyambungan hendaklah dibuat oleh pembekal di bawah pengawasan dan kawalaan pentadbir rangkaian UTM.

ii. Sebarang penyambungan rangkaian ke Intranet LPHS yang tidak mendapat kebenaran daripada UTM dalah menyalahi peraturan dan UTM berhak memutuskan penyambungan tersebut.

iii. Penyambungan Rangkaian Antara Bahagian (LAN) dan Rangkaian Luas (WAN) tidak boleh dilakukan oleh pengguna tanpa mendapat kelulusan daripada LPHS.

iv. Setiap projek pembinaan baru, penaik taraf bangunan dan kawasan baru mestilah mengambil kira keperluan semasa Teknologi Maklumat daripada UTM. Kos pemasangan infrastruktur rangkaian perlu dimasukkan dalam kos peruntukan pembinaan bangunan.

2.4 Kemudahan ICT

A. Pengenalan

Dasar ini menentukan penggunaan perkhidmatan Internet dan atau Intranet oleh pengguna bersesuaian sepertimana yang dikehendaki oleh LPHS. Dasar ini juga bertujuan melahirkan pengguna Internet yang beretika selaras dengan fungsi LPHS sebagai sebuah Institusi perumahan yang cemerlang.

B. Skop Dasar

Skop dasar adalah merangkumi:

a. Penggunaan kemudahan email Kerajaan Negeri dan bukan Kerajaan Negeri. Dasar ini terbahagi kepada dua bahagian, iaitu Dasar Am dan Dasar Khusus email;

b. Pembangunan laman web LPHS, sama ada dibangunkan secara berpusat (oleh Pengurus Laman WEB LPHS menggunakan pelayan web utama) atau secara bebas oleh unit; dan

c. Penggunaan Internet/ Intranet termasuk capaian sistem aplikasi LPHS, portal LPHS, laman web, pemindahaan data atau maklumat dan perbincangan melalui '*list group*' atau '*chat room*'.

C. Prosedur Piawaian Operasi

a. Penggunaan Email

i. Pihak SUK bertanggungjawab untuk menyediakan alamat email kepada semua kakitangan berdasarkan permohonan yang diluluskan oleh Setiausaha Bahagian, Bahagian Teknologi Maklumat, SUK Selangor melalui Ketua Pengarah Eksekutif LPHS.

ii. Segala polisi, peraturan dan dasar rujuk kepada DKICT Pejabat Setiausaha Kerajaan Negeri Selangor.

iii. Permohonan perlu dibuat dengan mengisi boring PKO/BTM/PPE-02 yang boleh dimuat turun di laman sesawang Setiausaha Kerajaan Negeri Selangor (http://www.selangor.gov.my)

b. Laman WEB

i. Ketua Unit/ kakitangan adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan maklumat yang dibekalkan kepada UTM. Pihak LPHS tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan. LPHS boleh menghadkan atau memansuhkan akses kepada tapak lama web tersebut berdasarkan keperluan semasa.

ii. Semua permohonan untuk pengemaskinian maklumat daripada unit perlu dikemukakan kepada UTM melalui memo (dalaman) dan semua salinan (*softcopy*) yang mengandungi maklumat unit/ persatuan dan sebagainya hendaklah dihantara ke UTM terlebih dahulu untuk disemak dan disahkan sebelum dimasukkan ke dalam server yang telah ditetapkan.

c. Maklumat Sulit/ Peribadi Pada Portal/ WEB

i. Sebarang penggunaan maklumat peribadi seseorang mestilah dinyatakan tujuannya dengan jelas dan mendapat kelulusan daripada Unit Sumber Manusia.

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 prosedur di dalam mahkamah, maka maklumat ini tidak termasuk di dalam Dasar ini iaitu:

- Bangsa
- Keturunan
- Agama, pandangan politik, ideology atau pun keahlian sesuatu persatuan
- Maklumat kesihatan, rawatan yang diambil

Nota:

- Semua maklumat yang sensatif hendaklah dinyatakan dengan jelas tujuan penggunaan data tersebut semasa permohonan mendapat meklumat 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 dengan 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 kepda seseorang yang laian 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.

d. Had-had Penggunaan

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

i. Had-had penggunaan untuk tujuan yang diperlukan penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat-syarat berikut:

- Tuan punya maklumat telah memberikan kebenaran menggunakan maklumat tersebut;
- Makumat boleh digunakan tuan punya maklumat bagi pengesahan sesuatu kontrak;
- Maklumat boleh digunakan untuk tujuan mahkamah atau perundangan; dan
- 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 ketik maklumat itu diambil, kebenaran daipada 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.

e. Penyenggaraan Maklumat Sulit / Peribadi

i. LPHS bertanggungjawab memastikan ketepatan maklumat peribadi, dan dikemaskini (jika perlu). Kemaskini maklumat diperlukan jika pemberi maklumat telah tamat perkhidmatan.

ii. LPHS bertanggungjawab menjamin keselamatan dan kerahsiaan maklumat yang disimpan.

iii. Data dienkrip sekiranya disimpan dalam media elektronik untuk penghantaran secara rangkaian.

iv. Permintaan untuk mencapai malumat 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.

v. Pihak LPHS berhak menggunakan maklumat peribadi untuk tujuan pengesahan atau bagi memenuhi keperluan LPHS, Negeri atau Negara.

vi. Pentadbir Sistem mestilah memahami dan mengikuti Dasar ini, dan bertanggungjawab untuk memaklumkan kepada pemberi maklumat tentang dasar ini.

D. Dasar e-mail

a. Dasar Am E-mail

i. Pengguna hendaklah mendaftar dan mengguna perisisan emel rasmi LPHS untuk tujuan komunikasi secara email.

ii. Aktiviti *spamming* atau *mail-bombing* dan penyebaran email dengan kandungan tidak beretika (seperti lucah, ugutan, perkauman, gangguan dan politik) kepada individu, *mailing list* atatu *discussion group* sama ada di dalam rangkaian Intranet LPHS atau ke Internet adalah tidak dibenarkan serta boleh diambil tindakan.

iii. Sebarang aktiviti komersial tanpa kelulusan LPHS adalah tidak dibenarkan.

iv. UTM/ BTM negeri berhak memasang sebarang jenis perisian atau perkakasan penapisan email dan virus (‘*email filter and antivirus*’) yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana email yang disyaki mengandungi virus atau berunsur *spamming* daripada memasuki ke dalam

server atau rangkaian Intranet LPHS dan keluar daripada pelayan (*server)* atau Intranet LPHS.

v. UTM/ BTM Negeri tidak bertanggungjawab terhadap pengguna yang menjadi penghantar (*sender*) atau penerima (*receiver*) kepada sebarang email yang berunsur '*spamming*' atau penyebaran emaial dengan kandungan tidak beretika.

vi. UTM/ BTM Negeri tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, data, kotak mail atau fail yang disimpan oleh pengguna di dalam server akibat daripada penggunaan perkhidmatan email.

b. Dasar Khusus

i. Kemudahan emel disediakan dan diberi kepada semua kakitangan yang berdaftar. Kemudahan email juga boleh disedia kepada organisasi atau persatuan rasmi LPHS melalui permohonan kepada UTM. Pengguna tidak dibenarkan untuk memohon penukaran alamat email.

ii. Seseorang pengguna individu tidak dibenarkan untuk memohon dan/ atau memiliki lebih daripada satu akuan atau alamat email LPHS pada satu-satu masa.

iii. Penggunaan nama samaran dalam alamat email adalah tidak dibenarkan.

iv. Setiap alamat email 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.

v. Pengguna dilarang menggunakan kemudahan email untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan dan undang-undang LPHS, negeri dan Negara.

vi. Semua pengguna tidak dibenarkan mengguna email luar untuk tujuan rasmi sekiranya email rasmi telah diberikan. Pentadbiran rangkiaian berhak menghalang penggunaan email tersebut jika didapati memudarat dan membebankan rangkaian Intranet LPHS.

vii. Dari semasa ke semasa atas sebab-sebab keperluan audit, keselamatan dan penggunaan, pentadbir email dengan kelulusan LPHS berhak

memeriksa, membuang dan melihat isi kandungan email dan ruang storan pengguna-pengguna

E. Dasar Pembangunan Laman WEB

a. LPHS menyediakan tapak untuk laman WEB rasmi jabatan/ persatuan atau aktiviti rasmi sahaja.

b. Semua pengguna yang ingin mula menggunakan perkhidmatan muat naik dan muat turun laman web rasmi jabatan/persatuan, hendaklah terlebih dahulu mengemukakan memo kepada UTM beserta salinan (*softcopy)* sebelum dikemaskini.

c. LPHS berhak menukar atau mengubahsuai alamat capaian dan kandungan laman web atas kepentingan LPHS berdasarkan keperluan semasa.

d. LPHS berhak menentukan perisian pembangunan laman WEB bagi tujuan pengoptimumkan penggunaan dan keselamatan.

e. Laman WEB peribadi yang berbentuk ilmiah adalah dibenarkan tetapi perlu mendapat kelulusan LPHS, Pihak LPHS tidak akan bertanggungjawab terhadaap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh jabatan atau persatuan.

f. Kandungan laman web mesti dipersembahkan dalam Bahasa Melayu. Penggunaan bahasa lain perlu mendapat kelulusan daripada LPHS.

g. Kandungan laman web hendaklah tidak mengandungi maklumat atau terdedah kepada kemasukan maklumat yang menyalahi undang-undang/ peraturan LPHS, negeri dan Negara termasuk kepada maklumat yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganaan, keruntuhan akhlak dan kebencian.

F. Dasar Capaian Internet dan/atau Intranet

a. LPHS berhak menyedia dan memasang perisian penapisan isi kandungan Intranet dan/ atau internet.

b. Laman-laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan. Laman yang berbentuk keganasan, lucah, hasutan, perkauman, membawa kepada keganasan, keruntuhan akhlak dan kebencian

adalah tidak dibenarkan sama sekali kecuali mendapat kelulusan daripada Setiausaha Bahagian, BTM Negeri melalui Ketua Pengarah Eksekutif.

c. Capaian laman yang berbentuk hiburan, hobi atau '*leisure*' tidak dibenarkan di waktu pejabat, termasuk laman '*game online*', '*radio online*' dan '*video streaming*' yang membebankan rangkaian intranet LPHS kecuali yang telah disediakan oleh UTM dengan kelulusan Setiausaha Bahagian, BTM Negeri.

d. Melayari internet tanpa tujuan atau meninggalkan capaian internet '*unattended*' adalah tidak dibenarkan kerana ianya menyebabkan kesesakan rangkaian intranet LPHS.

e. LPHS berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yagn dianggap tidak sesuai.

f. Pengguna dilarang mengganggu atau menceroboh laman web mana-mana jabatan, organisasi, negeri dan Negara.

g. Pengguna dilarang memasuk, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada internet yang menyalahi undang-undang Negara.

h. '*Internet chatting*' tidak dibenarkan. Penggunaan untuk tujuan rasmi perlu mendapat kelulusan daripada Setiausaha Bahagian, BTM Negeri secara bertulis melalui ketua Ketua Pengarah Eksekutif, LPHS. Permohonan hendaklah menyatakan tujuan penggunaan, senarai pengguna dan perisian yang digunakan.

i. Kebenaran '*chatting intranet*' adalah berdasarkan kelulusan UTM.

j. Pengguna tidak dibenarkan menggunakan sumber ICT LPHS untuk menggodam mana-mana sistem komputer sama ada di dalaam atau di luar LPHS. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem-sistem komputer tersebut atau mencapai sumber ICT LPHS dengan menggunakan identity pengguna lain.

k. Pengguna tidak dibenarkan mencapai atau cuba mencapai sumber elektrinik (data, paparan, '*keystroke*', fail atau media storan) dalam sebarang bentuk yang dimiliki oleh pengguna yang laintanpa 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.

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

2.5 Akauntabiliti dan Kerahsiaan Maklumat

A. Pengenalan

Dasar ini menyatakan tanggungjawab pihak yang terlibat degan penggunaan kemudahan ICT di LPHS mencakupi perkara-perkara berikut:

a. Melindungi kepentingan pengguna ICT apabila berlaku pelanggaran atau pencabulan Dasar Keselamat ICT;

b. Melindungi semua data dan maklumat milik LPHS;

c. Membantu usaha LPHS untuk menjaga kepentingan pihak-pihak yang berkepentingan (*stakeholdes*); dan

d. Menjelaskan tanggungjawab pentadbir operasi yang melibatkan capaian data, maklumat atau kegiatan pengguna yang diklasifikasikan sebagai rahsia atau sulit.

B. Skop Dasar

Skop dasar ini meliputi tanggungjawab pengguna dan LPHS yang berkaitan capaian maklumat sulit kecuali maklumat peribadi yang diambil untuk memudahkan seseorang individu berhubung, seperti alamat yand disediakan oleh seseorang individu.

C. Dasar Capaian Maklumat Sulit

a. Pengguna tidak dibenarkan menyimpan data atau maklumat yang dikategorikan sebagai *sensitive*, rahsia dan sulit.

b. Pentadbiran sistem berhak untuk mencapai, merekod atau memantau data, maklumat atau kegiatan pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT. Maklumat-maklumat ini hanya boleh digunakan untuk tujuan penjagaan keselamatan ICT.

c. Pentadbir sistem berhak memantau kegiatan dan aktiviti pengguna yang melanggar Dasar Keselamatan ICT. Segala maklumat yang direkod boleh digunakan sebagai bukti pelanggaran Dasar Keselamatan ICT. Sekiranya pelanggaran dasar itu serius seperti menggunakan pengenalan (*identity)*

pengguna lain untuk mencuri data atau merosakkan sumber ICT, maka bukti-bukti yang dikumpul boleh dimajukan kepada Jawatankuas ICT LPHS.

d. Pentadbir operasi boleh membuat salinan dalam bentuk bercetak atau digital sebagai bahan bukti. Pentadbir sistem dengan kebenaran bertulis LPHS boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti email atau fail-fail yang tersimpan dalam akaunnya.

e. Pengguna diberi jaminan bahawa selain daripada perkara-perkara yang disebutkan diatas, data atau maklumat rahsia atau sulit yang terdapat dalam akaun pengguna tidak boleh dicapai oleh sesiapa pun. Sesiapa yang mencapai data atau maklumat pengguna lain tanpa kebenaran, maka individu tersebut dianggap telah melanggar Dasar Akauntabiliti dan Kerahsiaan Maklumat dan boleh dikenakan tindakan tatatertib.

D. Dasar Pemantauan Data dalam Rangkaian

a. Pentadbir sistem berkuasa untuk memantau dan merekodkan data-data yang berada dalam rangkaian sebagai sebahagian daripada rutin penjagaan keselamatan sumber ICT. Jaminan diberikan bahawa data-data yang direkodkan tidak akan didedahkan melainkan untuk tujuan penyiasatan sekiranya berlaku kejadian pelanggaran Dasar Keselamatan ICT LPHS.

b. Sekiranya pentadbir operasi mengesyaki pengguna melanggar Dasar Keselamatan ICT, pentadbir operasi mempunyai mandat untuk memantau dan merekodkan data-data dalam talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data ini akan digunakan sebagai bahan bukti untuk proses pengauditan yang akan dilakukan oleh Jawatankuasa ICT.

c. Adalah menjadi kesalahan jika pengguna selain daripada pegawai yang diberi kuasa memantau atau merekodkan data yang berada dalam rangkaian kecuali untuk perkara-perkara yang dinyatakan di atas.

2.6 Keselamatan ICT

A. Pengenalan

Dasar ini bertujuan untuk:

i. Memastikan pengawalan dan pengurusan keselamatan perkakasan, perisian, aplikasi dan operasi komputer; dan

ii. Menerangkan pelaksanaan keselamatan rangkaian Intranet LPHS yang merupakan satu infrastruktur rangkaian setempat (LAN) untuk penyambungan bagi tujuan komunikasi dan perkongsian maklumat/ sumber.

B. Skop Dasar

Skop dasar merangkumi:

i. Aspek keselamatan perkakasan, perisian sistem, pangkalan data dan sistem aplikasi; dan

ii. Aspek rekabentuk keselamatan rangkaian.

C. Prosedur Piawaian Operasi

1. Keselamatan Sistem Komputer dan Server

i. Kawalan Capaian Logikal

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 wujudnya kemudahan menyemak semua aktiviti pengguna untuk tujuan pengauditan;

d. Memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan bertulis dan memastikan tiada ID yang tidak mempunyai pengguna; dan

e. Perubahan ID pengguna untuk sistem aplikasi perlu mendapat kebenaran bertulis daripada pemilik (*owner*) sistem tersebut.

ii. Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan, pentadbir sistem berhak:

a. Menggantung semua kemudahan (*privillage*) ID yang berkaitan; dan

b. Menghapus semua kemudahan untuk pengguna yang tamat perkhidmatan 330 hari selepas tarikh tamat perkhidmatan.

c. Jejak Audit (*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 berlaku pencerobohan ke atas maklumat.

iii. Autentikasi Pengguna

a. Autentikasi pengguna bertujuan mengenalpasti hanya pengguna yang sah dibenarkan mengggunakan 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 atau symbol-simbol lain;
- Kata laluan di enkripsi semasa penghantaran;
- Fail kata laluan disimpan berasingan daripada data sistem aplikasi utama; dan
- Cubaan capaian dihadkan kepada tiga (3) kalai sahaja. ID pengguna berkenaan akan digantung selepas tiga (3) kali cubaan gagal yang berturut. Penggantungan hanya boleh dibatalkan dengan mengemukakan permohonan bertulis kepada pentadbir sistem.

iv. Jejak audit (*Audit trail*)

a. Maklumat '*audit trail*' merangkumi:

- Identifikasi (ID) pengguna;

- Fungsi sumber dan maklumat yang digunakan atau dikemaskini;
- Tarikh dan masa penggunaan;
- Alamat IP '*client*'; dan
- Sebarang transaksi yang dilakukan.

b. LPHS berhak mengambil tindakan berikut semasa penyediaan jejak audit (*audit trail*):

- Menyemak dan melaporkan sebarang aktiviti yang diragui dengan segera;
- Menyemak jejak audit (*audit trail*) secara berjadual;
- Menyemak dan melaporkan sebarang masalah keselamatan dan kejadian luar biasa;
- Menyimpan maklumat jejak audit (*audit trail*) untuk jangka masa tertentu bagi keperluan operasi dan keselamatan; dan
- Mengawal maklumat jejak audit (*audit trail*) daripada dihapus, diubahsuai, ditipu atau disusun semula.

v. Penyalinan (backup) Maklumat

LPHS akan mengambil tindakan berikut semasa penyediaan penyalinan:

a. Mendokumen tatacara prosedur penyalinan dan pemulihan;

b. Menyimpan dua (2) medium salinan; dan

c. Menguji medium salinan dan tatacara prosedur pemulihan sekurang-kurangnya dua (2) kali setahun.

vi. Penyenggaraan

a. '*Patches*' dan Kelemahan Sistem (*Vulnerabilities*)

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

b. Peningkatan (*upgrade*)

Menaiktaraf sistem pengoperasian kepada versi terkini.

2. Keselamatan Sistem Komputer dan Server

i. Perisian aplikasi

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

- Sistem keselamatan berpusat dengan kawalan capaian penggunaan satu ID dan kata laluan untuk semua aplikasi yang berkaitan;
- Profil capaian yang menghad tahap capaian maklumat serta fungsi-fungsi berdasarkan peranan pengguna;
- Kawalan peringkat sistem aplikasi yang menentukan akauantabiliti tertentu kepada pengguna; dan
- Penetapan pemilik (*ownership*) maklumat.

ii. Pangkalan Data

LPHS bertanggungjawab mengadakan kawalan capaian kepada pangkalan data. Integriti maklumat yang disimpan di dalam pangalan data dikekal dan dijamin secara:

- Sistem pengurusan pangkalan data memastikan integriti dalam pengemaskinian dan capaian maklumat; dan

- Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data.

iii. Pengujian Aplikasi

LPHS bertanggungjawab menguji atucara, modul, sistem aplikasi dan integrasi sistem aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan.

LPHS mengambil langkah berikut semasa pengujian aplikasi:

- Menggunakan data ujian (*dummy*) atau data lapuk (*historical*);
- Mengawal penggunaan data terpilih (*classified*);
- Menghadkan capaian kepada kakitangan yang terlibat sahaja;
- Menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk); dan
- Menggunakan persekitaran yang berasingan untuk pembangunan dan pengoperasian sistem aplikasi.

iv. Perisian Berkod Jahat (*malicious*) dan rosak (*defective*)

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

- Mendapat kod sumber (*source code*) daripada pembangun sistem aplikasi yang bereputasi baik, rekod prestasi perkhidmatan yang baik dan mempunyai kepakaran teknikal yang tinggi;
- Mewujud dan melaksana program jaminan kualiti dan prosedur untuk semua sistem aplikasi yang dibangunkan secara dalaman dan luaran; dan
- Memastikan semua sistem aplikasi didokumen, diuji, disah fungsinya, tahan lasak (*robustness*) dan menepati spesifikasi.

v. Perubahan Versi (*version*)

LPHS bertanggungjawab mengawal versi sistem aplikasi apabila perubahan atau peningkatan dibuat dan mematuhi prosedur kawalan perubahan.

vi. Penyimpanan Kod Sumber (source code)

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

- Mewujudkan prosedur penyenggaraan versi terkini; dan
- Mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada

vii. Kawalan Kod Jahat (*malicious code*)

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

- Melaksanakan prosedur untuk mengurus kod jahat;
- Mewujudkan peraturan berkaitan memuat turun, penerimaan dan penggunaan perisian percuma (freeware dan shareware);
- Menyebarkan arahan dan maklumat untuk mengesan kod jahat kepada semua pengguna; dan
- Mengambil langkah pencegahan atau pemulihan serangan kod janat seperti berikut:
    - Mengimbas dan menghapus kod jahat menggunakan perisian anti virus yang diluluskan LPHS;
    - Menyemak status proses imbasan dalam laporan log; dan
    - Tidak melaksakan (*run*) atau membuka fail kepilan (*attachment*) daripada email yang meragukan.

D. Dasar keselamatan sistem Aplikasi

LPHS bertanggungjawab melaksana dan mengawal tahap capaian sistem aplikasi.

E. Dasar keselamatan Sustem Komputer dan Pelayan

1. Kawalan Capaian Fizikal

   i. Kawalan terhadap individu/ kakitangan yang memasuki Bilik Operasi Komputer dan kawalan akses kepada komputer pelayan serta sumber-sumber ICT lain; dan

   ii. Mewujudkan prosedur kawalan capaian fizikal terhadap komputer pelayan bagi individu/ kakitangan.

2. Kawalan Capaian Logikal

   Kawalan dibuat semasa instalasi. Hanya mereka yang dibenarkan sahaja boleh mencapai sistem dan mekanisma kawalan capaian adlaah seperti berikut:

   - Identifikasi Pengguna

     Pengguna sistem boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akauan kumpulan pengguna yang sama.

3. Jejak Audit

   LPHS bertanggungjawab menyedia dan menyimpan rekod jejak audit bagi mengenalpasti akauntabiliti pengguna dan keselamatan data. Jejak audit untuk sistem komputer dan manual operasi perlu diwujudkan bagi:

   - Capaian kepada maklumat yang kritikal;
   - Capaian kepada perkhidmtan rangkaian; dan
   - Kebenaran istimewa kepada pengguna biasa digunakan seperti arahan-arahan keselamatan dan fungsi-fungsi '*superuser*'.

4. Penyalinan (backup) Maklumat

   i. LPHS bertanggungjawab memulihkan sistem sepenuhnya jika berlaku masalah atau kerosakan.

   ii. Proses penyalinan hendaklah dibuat secara berjadual dan semasa membuat sebarang perubahan konfigurasi pada sistem. '*Backup*' perlu disimpan dengan baik di tempat yang selamat.

5. Penyelenggaraan

   LPHS akan melaksanakan kawalan dan penyelenggaraan bagi memastikan integriti sistem pengoperasian tidak terdedah kepada sebarang pencerogohan keselamatan.

F. Dasar Keselamatan Penggunaan Email

- Akaun email

  Akaun email bukan hak mutlak tetapi merupakan kemudahan yang disediakan tertakluk kepada peraturan LPHS/ negeri dan boleh ditarik balik jika melanggar Dasar Internet/ Intranet.

G. Dasar Keselamatan Peralatan Rangkaian

1. Keselamatan Fizikal

   i. Peralatan rangkaian hendaklah ditempatkan di tempat khas yang bebas daripada risiko di luar jangka seperti banjir, kilat, gegaran, bencana alam dan sebagainya.

   ii. Suhu hendaklah terkawal di dalam had suhi 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*) sercer secara otomatik.

   iv. Sebarang akses ke dalam bilik server hanya kepada kakitanganf yang dibenarkan sahaja. Hanya pelawat yang dibenarkan boleh memasuki bilik server dengan pengawasan kakitangan UTM.

2. Capaian Fizikal

   i. Capaian Pengkabelan Rangkaian

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

- Melindungi pengkabelan di dalam kawasan awam dengan cara memasang *conduit* atau lain-lain mekanisma perlindungan yang sesuai; dan

- Pusat pendawaian terletak di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

ii. Capaian Peralatan Rangkaian

Capaian peralatan rangkaian hendaklah:

- Ditempatkan di tempat yang selamat, terkawal; dan

- Hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

3. Capaian Logikal

i. ID dan kata lalaun 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.

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.

v. Perubahan perisian konfigurasi mestilah direkodkan – pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.

4. Penggunaan Peralatan Tanpa Kebenaran

    i. Mengadakan kawalan capaian logikal seperti yang disebut di para 8.6.3.

    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.

5. Konfigurasi Peralatan

    i. Mengaktifkan (*enable*) perkhidmatan yang diperlukan sahaja.

    ii. Menghadkan capaian konfigurasi kepada noe atau alamat IP yang dibenarkan sahaja.

    iii. Mematikan (*disable*) penyiaran trafik (*broadcast*).

    iv. Menggunakan kata laluan yang selamat dan tidak mudah di cerobohi.

    v. Dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.

6. Penyenggaraan Peralatan

    i. Peralatan hendaklah dipasang, dioperasi dan diselenggaraa mengikut spesifikasi pengilang.

    ii. Dibaiki dan diselneggara hanya oleh kakitangan yang terlatih dan dibenarkan sahaja.

    iii. Mengemaskini rekod penyenggaraan.

H. Dasar kebolehcapaian Pengguna (*User Accessibility*)

1. Rangkaian setempat (*local are network*)

    - Hanya kakitangan dan pelajar LPHS dibenarkan membuat penyambungan ke rangkaian Intranet LPHS (rujuk Dasar Rangkaian)

- Pengguna luar perlu mendapatkan kebenaran daripada UTM sebelum membuat capaian kepada sistem pengkomputeran LPHS.

- Perisisan penguntip (*sniffer*) atau penganalisis rangkaian (*network analyzer*) tidak dibenar digunakan pada sebarang komputer kecuali setelah mendapat kebenaran daripada LPHS. Status komputer hendaklah disemak setiap tahun.

- Setiap komputer hendaklah dipasangkan dengan perisian antivirus, *anti-spyware*, anti-malware dan anti-adware yang dibekalkan oleh UTM/ negeri.

I. Dasar Sambungan Dengan Lain-lain Rangkaian

1. Capaian Yang Tidak Digalakkan

   - Penggunaan protocol rangkaian seperti NetBios dan IPX/SIPX

   - Penggunaan workgroup kerana menyokong '*share-level security*'

2. Firewall

   Semua trafik rangkaian daripada dalam ke luar LPHS dan sebaliknya mestilah melalui *firewall* dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya berasaskan kepada Dasar Rangkaian.

Lampiran 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR

Nama (Huruf Besar) : ----------

No Kad Pengenalan : ----------

Jawatan : ----------

Bahagian : ----------

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa: -

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT LEMBAGA PERUMAHAN DAN HARTANAH SELANGOR; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan :

Tarikh :

Pengesahan Pengarah Eksekutif.

…….
(Nama Pengarah Eksekutif)
Pengarah Eksekutif
Lembaga Perumahan Dan Hartanah Selangor.

Tarikh : …….

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan
b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”
c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)
d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)”
e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”
f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Pandunan Penilaian Risiko Keselamatan Maklumat Sektor Awam
g. Akta Tandatangan Digital 1997
h. SPA Bilangan 4 Tahun 2006
i. Akta Rahsia Rasmi 1972
j. Akta Jenayah Komputer 1997
k. Akta Hak cipta (Pindaan) Tahun 1997
l. Akta Komunikasi dan Multimedia 1998
m. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- “Tatacara Penyediaan, Penilaian dan Penerimaan Tender”
n. Surat Pekeliling Perbendaharaan Bil.3/1995 – “Peraturan Perolehan Perkhidmatan Perundingan”
o. Surat Pekeliling am Bil. 4 Tahun 2006 – “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam”
p. Perintah-perintah Am
q. Arahan Perbendaharaan
r. Arahan Teknologi Maklumat 2007
s. Surat akujanji
t. MPK Bahagian
u. Fail Meja Kakitangan
v. Pelan Kesinambungan Perkhidmatan, dan
w. Garis Panduan Penggunaan Mel Elektronik Pejabat SUK Selangor