DASAR KESELAMATAN ICT (DKICT)

Versi 1.2



PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR

TARIKH BERKUATKUASA : 18 OGOS 2014

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
14 Mei 2014	1.2	JPICT Bil. 2/2014	18 Ogos 2014
23 Januari 2013	1.1	JPICT Bil. 1/2013	05 Februari 2013
04 Oktober 2010	1.0	JPICT Bil. 4/2010	12 November 2010

JADUAL PINDAAN DASAR KESELAMATAN ICT PEJABAT SUK SELANGOR

TARIKH	VERSI	BUTIRAN PINDAAN
14 Mei 2014	**1.2**	**i.** **Perkara 020106 Pentadbir rangkaian,** muka surat 25: Penambahan klausa (g) iaitu : Penggunaan telefon mudah alih bagi tujuan *tethering modem* adalah DILARANG sama sekali. **ii.** **Perkara 070203 Pengurusan kata laluan,** muka surat 74 Pindaan pada klausa (c) kepada Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) dan perlu mengandungi gabungan huruf besar dan kecil **iii.** **Perkara 110105 Pelanggaran Perundangan,** muka surat 91 **:** Penambahan klausa seperti berikut:- SUB (BTM) atau ICTSO adalah berhak untuk mengambil tindakan sebagaimana berikut:- i) Membuat teguran pertama melalui e-mel, sistem pemantauan atau mana-mana medium komunikasi secara atas talian; ii) ICTSO akan memberi e-mel/surat teguran kepada pesalah dan satu salinan emel akan turut diberi kepada Ketua Jabatan/pegawai pesalah; iii) Pesalah hendaklah memberi surat tunjuk sebab dalam tempoh tiga (3) hari bekerja dari tarikh e-mel/surat diterima; dan iv) SUB (BTM) atau ICTSO berhak mengambil tindakan berupa menarik balik kemudahan capaian internet/peralatan ICT/komputer (sementara/kekal) bergantung kepada jenis dan tahap kesalahan.

ISI KANDUNGAN

PENGENALAN **8**
OBJEKTIF **8**
PENYATAAN DASAR **9**
SKOP **10**
PRINSIP-PRINSIP **13**
PENILAIAN RISIKO KESELAMATAN ICT **16**
BIDANG 01 ..... **17**
PEMBANGUNAN DAN PENYELENGGARAAN DASAR **17**
0101 Dasar Keselamatan ICT 17
010101 Pelaksanaan Dasar 17
010102 Penyebaran Dasar 17
010103 Penyelenggaraan Dasar 17
010104 Pengecualian Dasar 18
BIDANG 02 ..... **19**
ORGANISASI KESELAMATAN **19**
0201 Infrastruktur Organisasi Dalaman 19
020101 Y.B. Setiausaha Kerajaan Negeri (Y.B. SUK) 19
020102 Ketua Pegawai Maklumat (CIO) 19
020103 Setiausaha Bahagian BTM / SUB (BTM) 20
020104 Pegawai Keselamatan ICT (ICTSO) 21
020105 Pentadbir Sistem 23
020106 Pentadbir Rangkaian 24
020107 Pentadbir Pangkalan Data 25
020108 Pentadbir Web 26
020109 Pengguna 27
020110 Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT) 28
020112 Jawatankuasa Tindak Balas Insiden Keselamatan ICT PEJABAT SUK SELANGOR (SUK CERT SELANGOR) 30
0202 Pihak Ketiga 31
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 31
BIDANG 03 ..... **33**
PENGURUSAN ASET **33**

0301 Akauntabiliti Aset....33
030101 Inventori Aset ICT....33
0302 Pengelasan dan Pengendalian Maklumat....34
030201 Pengelasan Maklumat....34
030202 Pengendalian Maklumat....34
BIDANG 04....36
KESELAMATAN SUMBER MANUSIA....36
0401 Keselamatan Sumber Manusia Dalam Tugas Harian....36
040101 Sebelum Perkhidmatan....36
040102 Semasa Perkhidmatan....37
040103 Program Kesedaran Keselamatan ICT....38
040104 Bertukar Atau Tamat Perkhidmatan....38
BIDANG 05....39
KESELAMATAN FIZIKAL DAN PERSEKITARAN....39
0501 Keselamatan Kawasan....39
050101 Kawalan Kawasan....39
050102 Kawalan Masuk Fizikal....40
050103 Kawasan Larangan....40
0502 Keselamatan Peralatan....43
050201 Peralatan ICT....43
050202 Media Storan....45
050203 Media Tandatangan Digital....46
050204 Media Perisian Dan Aplikasi....47
050205 Pelupusan....47
050206 Penyelenggaraan Perkakasan....49
050207 Peralatan di Luar Premis....50
0503 Keselamatan Persekitaran....50
050301 Kawalan Persekitaran....50
050302 Bekalan Kuasa....51
050303 Kabel....52
050304 Prosedur Kecemasan....52
0504 Keselamatan Dokumen....52
BIDANG 06....54
PENGURUSAN OPERASI DAN KOMUNIKASI....54
0601 Pengurusan Prosedur Operasi....54

060101 Pengendalian Dokumen Prosedur Operasi 54
060102 Kawalan Perubahan 54
060103 Pengasingan Tugas dan Tanggungjawab 55
060104 Prosedur Pengurusan Insiden 55
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 56
060201 Perkhidmatan Penyampaian 56
0603 Perancangan dan Penerimaan Sistem 57
060301 Perancangan Kapasiti 57
060302 Penerimaan Sistem 57
0604 Perisian Berbahaya 58
060401 Perlindungan dari Perisian Berbahaya 58
060402 Perlindungan dari *Mobile Code* 59
0605 *Housekeeping* 59
060501 *Backup* 59
0606 Pengurusan Rangkaian 60
060601 Kawalan Infrastruktur Rangkaian 60
0607 Pengurusan Media 62
060701 Media Mudah Alih 62
060702 Prosedur Pengendalian Media 62
060703 Keselamatan Sistem Dokumentasi 63
0608 Pengurusan Pertukaran Maklumat 63
060801 Pertukaran Maklumat 63
060802 Pengurusan Mel Elektronik (E-mel) 64
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*) 66
060901 E-Dagang 66
060902 Maklumat Umum 67
0610 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat 67
0611 Pemantauan 68
061101 Pengauditan dan Forensik ICT 68
061102 Jejak Audit 69
061103 Sistem Log 70
061104 Pemantauan Log 70
BIDANG 07 72
KAWALAN CAPAIAN 72

0701 Dasar Kawalan Capaian 72
070101 Keperluan Kawalan Capaian 72
0702 Pengurusan Capaian Pengguna 72
070201 Akaun Pengguna 72
070202 Hak Capaian (*Privilege*) 73
070203 Pengurusan Kata Laluan 73
070204 *Clear Desk* dan *Clear Screen* 74
0703 Kawalan Capaian Rangkaian 75
070301 Capaian Rangkaian 75
070302 Capaian Internet 76
0704 Kawalan Capaian Sistem Pengoperasian 77
070401 Capaian Sistem Pengoperasian 77
0705 Kawalan Capaian Aplikasi dan Maklumat 79
070501 Capaian Aplikasi dan Maklumat 79
0706 Peralatan Mudah Alih dan Jarak Jauh 80
070601 Peralatan Mudah Alih 80
070602 Kerja Jarak Jauh 80
BIDANG 08 81
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 81
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi 81
080101 Keperluan Keselamatan Sistem Maklumat 81
080102 Pengesahan Data *Input* dan *output* 81
080103 Kawalan Prosesan 82
0802 Kawalan Kriptografi 82
080201 Enkripsi 82
080202 Tandatangan Digital 82
080203 Penggunaan Infrastruktur Kunci Awam (PKI) 82
0803 Keselamatan Fail Sistem 82
080301 Kawalan Fail Sistem 83
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem 83
080401 Prosedur Kawalan perubahan 83
080402 Pembangunan Perisian Secara *Outsource* 84
0805 Kawalan Teknikal Keterdedahan (*vulnerability*) 84
080501 Kawalan dari Ancaman Teknikal 84
BIDANG 09 85

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 85
0901 Mekanisme Pelaporan Insiden Keselamatan ICT 85
090101 Mekanisme Pelaporan 85
0902 Pengurusan Maklumat Insiden Keselamatan ICT 87
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 87
BIDANG 10 88
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 88
1001 Dasar Kesinambungan Perkhidmatan 88
100101 Pelan Pengurusan Kesinambungan Perkhidmatan 88
BIDANG 11 90
PEMATUHAN 90
1101 Pematuhan dan Keperluan Perundangan 90
110101 Pematuhan Dasar 90
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 90
110103 Pematuhan Keperluan Audit 90
110104 Keperluan Perundangan 91
110105 Pelanggaran Perundangan 91
Glosari 92
Lampiran 1 99
Lampiran 2 100
Lampiran 3 102

PENGENALAN

Pejabat Setiausaha Kerajaan Negeri Selangor (PEJABAT SUK SELANGOR) berperanan untuk menyediakan perkhidmatan bagi perancangan, pembangunan dan pengurusan sumber manusia sektor awam yang cemerlang berteraskan profesionalisme, integriti dan teknologi. Dokumen ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dan melindungi aset ICT Pejabat SUK Selangor. Dokumen ini diguna pakai oleh semua pihak kakitangan, pengguna dan pembekal yang menyediakan perkhidmatan, mencapai dan menggunakan aset dan sistem aplikasi ICT di PEJABAT SUK Selangor.

OBJEKTIF

Dasar Keselamatan ICT (DKICT) SUK Selangor diwujudkan untuk menjamin kesinambungan urusan SUK Selangor dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama DKICT di PEJABAT SUK 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(*CIA*^{3});

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 PEJABAT SUK SELANGOR; dan

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

PENYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan 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 PEJABAT SUK 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 PEJABAT SUK SELANGOR merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan/atau kertas bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

1) **Kerahsiaan** – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan 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 ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap 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 PEJABAT SUK SELANGOR terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT, perkhidmatan dan data. DKICT PEJABAT SUK 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 dengan 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 PEJABAT SUK SELANGOR, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, DKICT PEJABAT SUK SELANGOR ini merangkumi perlindungan ke atas semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, 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 PEJABAT SUK SELANGOR. Contoh peralatan dan periferal seperti komputer, pelayan, *firewall,* pencetak, peralatan media, peralatan komunikasi dan alat-alat prasarana seperti *Uninterruptible Power Supply (UPS)* dan sebagainya;

2) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan

sistem pengoperasian komputer yang disimpan di dalam 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 PEJABAT SUK 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 pencegah kebakaran dan lain-lain.

4) Data dan maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PEJABAT SUK SELANGOR. Contohnya sistem dokumentasi, prosedur operasi, rekod-rekod PEJABAT SUK SELANGOR, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

5) Manusia

Semua pengguna infrastruktur ICT PEJABAT SUK SELANGOR yang dibenarkan, termasuk kakitangan, pengguna dan pembekal. Individu yang mempunyai pengetahuan untuk melaksanakan skop kerja harian PEJABAT SUK SELANGOR bagi mencapai misi dan objektif jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

6) Media storan

Semua media storan dan peralatan yang berkaitan seperti disket, storan mudah alih, 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 perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT PEJABAT SUK SELANGOR dan perlu dipatuhi adalah seperti berikut:

1) Akses Atas Dasar Perlu Mengetahui

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

2) Hak Akses Minimum

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

3) Kebertanggungjawaban/Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii) Menentukan maklumat sedia untuk digunakan;

iv) Menjaga kerahsiaan kata laluan;

v) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

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

vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

4) Pengasingan

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

5) Pengauditan

Tujuan aktiviti ini ialah untuk mengenalpasti insiden berkaitan keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router, firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau Jejak audit (*audit trail)*. Semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit;

6) Pematuhan

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

7) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses penduaan (*backup*) dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan (BRP); dan

8) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

PEJABAT SUK SELANGOR hendaklah melaksanakan penilaian risiko Keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat PEJABAT SUK SELANGOR termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses,prosedur serta kakitangan. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan yang lain.

PEJABAT SUK 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.

PEJABAT SUK 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 kriteria yang telah ditetapkan oleh pengurusan agensi;

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

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

BIDANG 01
PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 Dasar Keselamatan ICT

Objektif :
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PEJABAT SUK SELANGOR yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Y.B. Setiausaha Kerajaan Negeri (Y.B. SUK) dibantu oleh Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT) yang terdiri daripada :- i) Ketua Pegawai Maklumat (CIO); ii) Setiausaha Bahagian (BTM); iii) Pegawai Keselamatan ICT (ICTSO);dan iv) Semua Ketua Bahagian.	Y.B. SUK; CIO

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna yang terlibat dengan infrastruktur ICT PEJABAT SUK SELANGOR meliputi kakitangan, pengguna dan pembekal.	ICTSO

010103 Penyelenggaraan Dasar

Dasar Keselamatan ICT PEJABAT SUK SELANGOR adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT PEJABAT SUK SELANGOR:	JPICT; ICTSO

a) Mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan, pertimbangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), PEJABAT SUK SELANGOR; c) Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pihak iaitu kakitangan, pengguna dan pembekal; dan d) Menyemak semula dokumen sekurang-kurangnya setahun sekali atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT PEJABAT SUK SELANGOR adalah terpakai dan mestilah dipatuhi oleh semua kakitangan, pengguna serta pembekal ICT PEJABAT SUK SELANGOR dan tiada pengecualian diberikan.	Semua

BIDANG 02
ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

Objektif:
Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT PEJABAT SUK SELANGOR.

020101 Y.B. Setiausaha Kerajaan Negeri (Y.B. SUK)

Peranan dan tanggungjawab Y.B. SUK adalah seperti berikut: a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PEJABAT SUK SELANGOR; b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PEJABAT SUK SELANGOR, c) Memastikan semua keperluan jabatan seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi, dan d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PEJABAT SUK SELANGOR;	Y.B. SUK

020102 Ketua Pegawai Maklumat (CIO)

Jawatan Ketua Pegawai Maklumat (CIO) adalah disandang oleh Timbalan Setiausaha Kerajaan Negeri (Pengurusan). Peranan dan tanggungjawab CIO adalah seperti berikut: a) Membantu Y.B. SUK dalam melaksanakan tugas-tugas yang berkaitan Keselamatan ICT; b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT PEJABAT SUK SELANGOR;	CIO

c) Bertanggungjawab menyelaras dan mengurus pelan tindakan dan program keselamatan seperti penyediaan DKICT PEJABAT SUK SELANGOR, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; d) Menentukan keperluan keselamatan ICT; dan e) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT PEJABAT SUK SELANGOR di semua bahagian di PEJABAT SUK SELANGOR (CIO).	
020103 Setiausaha Bahagian BTM / SUB (BTM)	
Peranan dan tanggungjawab SUB (BTM) adalah seperti berikut: a) Memastikan DKICT PEJABAT SUK SELANGOR dilaksanakan di bahagian; b) Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan bahagian mematuhi dasar, piawaian dan garis panduan keselamatan ICT dan seterusnya melaporkan sebarang insiden berkaitan keselamatan ICT; c) Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu; d) Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i) Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii) Pembelian atau peningkatan perisian dan sistem komputer; iii) Perolehan teknologi dan perkhidmatan komunikasi baru; dan iv) Pelantikan pembekal, perunding atau rakan usaha sama. e) Menyimpan rekod atau laporan terkini tentang ancaman keselamatan. Sebarang perkara atau penemuan ancaman terhadap keselamatan ICT hendaklah dilaporkan kepada ICTSO;	SUB (BTM)

f) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT PEJABAT SUK SELANGOR; g) Membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT di bahagian; h) Melaksanakan sistem kawalan capaian pengguna ke atas aset-aset ICT PEJABAT SUK SELANGOR; i) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PEJABAT SUK SELANGOR; j) Menentukan kawalan akses pengguna terhadap aset ICT PEJABAT SUK SELANGOR; k) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; l) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PEJABAT SUK SELANGOR.	
020104 Pegawai Keselamatan ICT (ICTSO)	
Jawatan Pegawai Keselamatan ICT (ICTSO) adalah disandang oleh Ketua Penolong Setiausaha (BTM). Peranan dan tanggungjawab ICTSO adalah seperti berikut: a) Mengurus keseluruhan program keselamatan ICT PEJABAT SUK SELANGOR; b) Memberi penerangan dan pendedahan berkenaan DKICT PEJABAT SUK SELANGOR kepada semua pengguna;	ICTSO

c) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT PEJABAT SUK SELANGOR.

d) Menjalankan pengurusan risiko;

e) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan PEJABAT SUK SELANGOR berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

g) Mencadangkan langkah-langkah pengukuhan bagi mematuhi dasar-dasar berkaitan keselamatan ICT PEJABAT SUK SELANGOR;

h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT) MAMPU dan seterusnya membantu dalam penyiasatan atau pemulihan;

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

j) Menjalankan program-program kesedaran mengenai keselamatan ICT;

k) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman kepada keselamatan ICT dan menyediakan khidmat nasihat serta langkah pemulihan yang bersesuaian;

l) Memastikan pematuhan DKICT PEJABAT SUK SELANGOR oleh pihak luaran seperti perunding, kontraktor dan pembekal yang mencapai dan menggunakan aset ICT PEJABAT SUK SELANGOR untuk tujuan penyelenggaraan, pemasangan, naik taraf dan sebagainya;

m) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; n) Memastikan DKICT PEJABAT SUK SELANGOR dikemas kini sesuai dengan perubahan teknologi, arahan jabatan dan ancaman-ancaman dari semasa ke semasa; dan o) Memastikan Pelan Strategik ICT PEJABAT SUK SELANGOR mengandungi aspek keselamatan ICT.	
020105 Pentadbir Sistem	
Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut: a) Memastikan ketepatan dan menyekat kebenaran capaian serta-merta apabila tidak lagi diperlukan atau melanggar DKICT PEJABAT SUK SELANGOR; b) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat PEJABAT SUK SELANGOR; c) Menentukan ketepatan dan kesempurnaan kawalan capaian pengguna berdasarkan kepada garis panduan keselamatan ICT PEJABAT SUK SELANGOR; d) Mengambil tindakan segera dan bersesuaian apabila dimaklumkan oleh bahagian sekiranya terdapat pegawai yang telah tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas; e) Memantau aktiviti pengguna yang diberi keutamaan capaian yang tinggi dan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT PEJABAT SUK SELANGOR;	Pentadbir Sistem

f) Memantau aktiviti capaian harian sistem aplikasi pengguna; g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; h) Menganalisa dan menyimpan rekod jejak audit; i) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan j) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
020106 Pentadbir Rangkaian	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di PEJABAT SUK SELANGOR beroperasi sepanjang masa; b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian PEJABAT SUK SELANGOR secara tidak sah seperti melalui peralatan *modem* dan *dial-up;*	Pentadbir Rangkaian

g) Penggunaan telefon mudah alih bagi tujuan *tethering modem* adalah DILARANG sama sekali; dan h) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	
020107 Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b) Memastikan pangkalan data boleh digunakan pada setiap masa; c) Melaksanakan pemantauan dan penyenggaraan yang berterusan ke atas pangkalan data; d) Melaksanakan proses *backup* dan *restoration* ke atas pangkalan data; e) Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; f) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; g) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan h) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data

020108 Pentadbir Web	
Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a) Memastikan kandungan laman web sentiasa sahih dan terkini; b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d) Menghadkan capaian Pentadbir Laman Web bahagian ke *web server*; e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal PEJABAT SUK SELANGOR; f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; i) Melaksanakan proses *backup* dan *restoration* secara berkala; dan j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	Pentadbir Web

020109 Pengguna

Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Pengguna warga PEJABAT SUK SELANGOR dan pihak ketiga perlu membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat PEJABAT SUK SELANGOR; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii) Menentukan maklumat sedia untuk digunakan; iv) Menjaga kerahsiaan kata laluan; v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; vi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Pengguna

f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h) Menandatangani Surat Akuan Pematuhan DKICT PEJABAT SUK SELANGOR sebagaimana **Lampiran 1**.	
020110 Jawatankuasa Pemandu ICT PEJABAT SUK SELANGOR (JPICT)	
Keanggotaan JPICT adalah seperti berikut: **Pengerusi** : CIO **Ahli** : (1) Semua Ketua Jabatan/Bahagian (2) ICTSO (3) Semua PSU (BTM) **Urusetia** : Bahagian Teknologi Maklumat, PEJABAT SUK SELANGOR. **Bidangkuasa** : i) Menentukan arah tuju keselamatan ICT PEJABAT SUK SELANGOR; ii) Menilai, melulus dan menguatkuasakan pelaksanaan DKICT PEJABAT SUK SELANGOR; iii) Memastikan pengauditan sistem ICT PEJABAT SUK SELANGOR dilaksanakan; iv) Meluluskan program dan aktiviti berkaitan keselamatan ICT PEJABAT SUK SELANGOR; v) Memastikan DKICT PEJABAT SUK SELANGOR selaras dengan Pelan Strategik Teknologi Maklumat (PSTM);	CIO

vi) Memantau ancaman-ancaman utama keselamatan ICT;

vii) Melaporkan insiden keselamatan yang telah berlaku dan tindakan yang telah diambil kepada pihak pengurusan PEJABAT SUK SELANGOR;

viii) Menyenggara dokumen DKICT PEJABAT SUK SELANGOR;

ix) Memantau tahap pematuhan DKICT PEJABAT SUK SELANGOR;

x) Menilai aspek teknikal keselamatan projek-projek ICT;

xi) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT;

xii) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;

xiii) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

xiv) Memastikan DKICT PEJABAT SUK SELANGOR selaras dengan dasar-dasar ICT Kerajaan semasa; dan

xv) Bekerjasama dengan SUK CERT SELANGOR untuk mendapatkan maklum balas dan insiden untuk tindakan penyelenggaraan DKICT PEJABAT SUK SELANGOR.

020112 Jawatankuasa Tindak Balas Insiden Keselamatan ICT PEJABAT SUK SELANGOR (SUK CERT SELANGOR)

SELANGOR CERT

Keanggotaan CERT SELANGOR adalah seperti berikut:

Pengarah : SUB (BTM)

Pengurus : KPSU (BTM) / ICTSO

Ahli :
(1) PSU Kanan (BTM);
(2) Semua PSU (BTM);
(3) PPTM Kanan (BTM);
(4) Semua PPTM (KnR), BTM Selangor;
(5) PPTM (KS), BTM Selangor; dan
(6) Semua PPTM (Daerah) Selangor.

Urusetia : BTM, PEJABAT SUK SELANGOR

Peranan dan tanggungjawab CERT SELANGOR adalah seperti berikut:

i) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;

ii) Merekod dan menjalankan siasatan awal insiden yang diterima;

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

iv) Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya; dan

v) Merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan.

0202 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi: a) Membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT PEJABAT SUK SELANGOR perlu berlandaskan kepada perjanjian kontrak; e) Mengenal pasti risiko ke atas keselamatan maklumat dan memastikan pelaksanaan kawalan yang sesuai ke atas maklumat tersebut; f) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, dan g) Akses kepada aset ICT PEJABAT SUK SELANGOR perlu berlandaskan perjanjian kontrak. Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut:	CIO; SUB (BTM); ICTSO; Pihak Ketiga

a. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga, perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

i) DKICT PEJABAT SUK SELANGOR;

ii) *Non-Disclosure Agreement*;

iii) Akta Kawasan Larangan dan Tempat Larangan 1959;

iv) Arahan Teknologi Maklumat 2007 (IT Instructions);

v) Perakuan Akta Rahsia Rasmi 1972; dan

vi) Hak Harta Intelek.

h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT PEJABAT SUK SELANGOR sebagaimana **Lampiran 1**.

BIDANG 03
PENGURUSAN ASET

0301 Akauntabiliti Aset

Objektif :
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset PEJABAT SUK SELANGOR.

030101 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa di kemas kini; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Memastikan semua pengguna mengesahkan aset ICT yang ditempatkan di PEJABAT SUK SELANGOR; d) Semua peraturan pengendalian aset hendaklah dikenal pasti, didokumen dan dilaksanakan; e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f) Sebarang perlanggaran hendaklah dilaporkan kepada Pegawai Aset / ICTSO.	Pentadbir Sistem dan Semua

0302 Pengelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada PEJABAT SUK SELANGOR. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad.	Pegawai Aset ICT dan Semua
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan;	Semua

e) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;

f) Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;

g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum;

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

i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

BIDANG 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif :

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

040101 Sebelum Perkhidmatan

Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT. Perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan PEJABAT SUK SELANGOR c) Memenuhi keperluan prosedur keselamatan (NDA) bagi pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan	Semua

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

040102 Semasa Perkhidmatan

Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT PEJABAT SUK SELANGOR dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan ditetapkan PEJABAT SUK SELANGOR; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pegawai dan kakitangan PEJABAT SUK SELANGOR secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan PEJABAT SUK SELANGOR; dan	Semua

d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia (BPSM), PEJABAT SUK SELANGOR atau Bahagian Teknologi Maklumat Selangor.	
040103 Program Kesedaran Keselamatan ICT	
Setiap pengguna di PEJABAT SUK SELANGOR perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga adalah penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT PEJABAT SUK SELANGOR.	SUB (BTM)
040104 Bertukar Atau Tamat Perkhidmatan	
Memastikan pertukaran atau tamat perkhidmatan pegawai dan kakitangan PEJABAT SUK SELANGOR, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diuruskan dengan teratur. Perkara yang perlu dipatuhi termasuk: a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;dan b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat, kemudahan proses maklumat dan semua akses berkaitan mengikut peraturan yang ditetapkan PEJABAT SUK SELANGOR dan/atau terma perkhidmatan.	SUB (BPSM); SUB (BTM) SUB (BKP)

BIDANG 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

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

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan larangan melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	CIO; Pejabat Ketua Pegawai Keselamatan Negeri Selangor,; SUB (KP) dan ICTSO

i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- a) Setiap pengguna PEJABAT SUK SELANGOR hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Semua pas keselamatan hendaklah diserahkan balik kepada PEJABAT SUK SELANGOR apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama PEJABAT SUK SELANGOR. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.	Y.B. SUK; CIO; SUB (BTM); SUB (KP)

Kawasan larangan di PEJABAT SUK SELANGOR adalah:

a) Bilik Y.A.B. Dato' Menteri Besar;

b) Bilik Y.B. SUK;

c) Bilik Y.Bhg. Timbalan SUK;

d) Dewan Persidangan Negeri;

e) Semua Bilik Pegawai Daerah;

f) Semua Bilik Ketua Bahagian;

g) Semua Pusat Data;

h) Semua Bilik Server;

i) Bilik NOC;

j) Semua Bilik Peralatan Keselamatan dan Rangkaian;

k) Semua Bilik Kebal;

l) Semua Bilik Fail;

m) Semua stor; dan

n) Mana-mana kawasan yang telah/akan diisytiharkan sebagai kawasan larangan.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut:

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

b) Akses adalah terhad kepada pegawai yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

c) Pemantauan dibuat menggunakan kamera CCTV atau lain-lain peralatan yang sesuai;

d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;

e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

f) Pelawat yang dibawa masuk mesti diiringi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;

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

h) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;

i) Memperkukuhkan dinding dan siling;

j) Menghadkan jalan keluar masuk;

k) Mengadakan kaunter kawalan;

l) Menyediakan tempat atau bilik khas untuk pelawat; dan

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

0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT PEJABAT SUK SELANGOR dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; c) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; d) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; e) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; h) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; i) Peralatan-peralatan kritikal perlu disokong oleh UPS;	Semua

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

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

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

m) Peralatan ICT yang hendak dibawa keluar dari premis PEJABAT SUK SELANGOR, perlulah mendapat kelulusan Pegawai Aset ICT atau Penyelaras IT Bahagian dan direkodkan bagi tujuan pemantauan;

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

o) Aset ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

p) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT;

r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pegawai Aset ICT untuk dibaik pulih;

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

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

u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*Administrator Password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; w) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *"OFF"* apabila meninggalkan pejabat; x) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan y) Memastikan plag dicabut daripada suis utama (*Main Switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media-media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, langkah-langkah berikut perlu diambil: a) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b) Bagi media yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan terlebih dahulu;	Semua

c) Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan (*data safe*) yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; f) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; g) Storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang lebih privasi dan tidak terbuka kepada umum. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; h) Akses dan pergerakan kepada media storan yang mempunyai data kritikal perlu direkodkan; i) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; dan j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Tandatangan Digital	
Sebarang media yang digunakan untuk tandatangan digital hendaklah mematuhi langkah–langkah berikut: a) Pengguna hendaklah bertanggungjawab sepenuhnya bagi perlindungan daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;	Semua

b) Tidak boleh dipindah-milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan selanjutnya mengikut Prosedur Pelaporan Insiden.	
050204 Media Perisian Dan Aplikasi	
Sebarang media yang digunakan sebagai media perisian dan aplikasi hendaklah mematuhi langkah–langkah berikut: a) Hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan; b) Sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran SUB (BTM); c) Lesen perisian (*registration code*, *serials*, *CD-keys*) perlu disimpan berasingan daripada *CD-ROM, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050205 Pelupusan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh PEJABAT SUK SELANGOR dan ditempatkan di PEJABAT SUK SELANGOR dan Pejabat-pejabat Daerah Negeri Selangor. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT dilupuskan dengan teratur: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran;	Semua Pegawai Aset ICT dan BTM PEJABAT SUK SELANGOR

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

c) Pegawai Aset ICT akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

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

e) Pegawai Aset ICT bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem e-Aset;

f) Pelupusan peralatan ICT boleh dilakukan secara berpusat/tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;

g) Peralatan-peralatan ICT yang akan dilupuskan hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

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

   i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *mother board* dan sebagainya;

   ii) Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian PEJABAT SUK SELANGOR; dan

   iii) Memindah keluar dari PEJABAT SUK SELANGOR mana-mana peralatan ICT yang hendak dilupuskan;

i) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. j) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara.	
050206 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada SUB (BTM).	Pegawai Aset ICT dan BTM PEJABAT SUK SELANGOR

050207 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis PEJABAT SUK SELANGOR adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan sebarang kehilangan peralatan adalah di bawah tanggungjawab individu yang membawa keluar peralatan tersebut.	Semua
0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT PEJABAT SUK SELANGOR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk perolehan, menyewa, mengubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada SUB (BTM) dan Ketua Unit, Unit Pengurusan Bangunan (UPB) / Pengurus Bangunan. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua

c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Jurutera Tempatan (KP); PSU (Operasi); PSU (KnR)

050303 Kabel	
Kabel komputer/rangkaian hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:- a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	ICTSO dan Pentadbir Rangkaian
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan MAMPU 2004; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut Jabatan.	Semua
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat PEJABAT SUK SELANGOR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	

Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; c) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f) Pelupusan dokumen hendaklah mengikut Prosedur Keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan g) Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan, disimpan dan dihantar secara elektronik.	Semua

BIDANG 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

060101 Pengendalian Dokumen Prosedur Operasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan . c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Pengubahsuaian melibatkan perkakasan, sistem pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran SUB (BTM), pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskinikan mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Semua

c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau sebaliknya; dan e) Setiap perubahan hendaklah dibuat dengan menggunakan Borang Kawalan Perubahan.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem
060104 Prosedur Pengurusan Insiden	
CERT SELANGOR menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari PRISMA atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut.	Semua

Laporan insiden kemudiannya dimaklumkan kepada GCERT. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang. CERT SELANGOR yang diketuai oleh SUB (BTM) akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *on-site*. Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan akan dihantar bagi mendapatkan maklum balas GCERT MAMPU. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT SELANGOR seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan (BCP) perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan BCP. Laporan insiden yang tidak memerlukan BCP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di **Lampiran 2.**	
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut:- a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;	Semua

b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem dan ICTSO
060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Kriteria ini hendaklah merangkumi perkara berikut:- a) Memenuhi kehendak dan keperluan pengguna; b) Menggunakan perisian pembangunan yang sah; c) Menggunakan teknologi terkini;	Pentadbir Sistem ICT, ICTSO dan SUB (BTM)

d) Memenuhi ciri-ciri keselamatan bagi mengelakkan risiko pencerobohan dan sebagainya; dan e) Memenuhi keperluan-keperluan teknologi semasa dan akan datang (Contoh : mampu menggunakan pelbagai platform, IPv6 *ready*)	
0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
060401 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, IDS dan IPS mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemas kini paten antivirus dengan yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;	PSU (KnR); Semua

f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem
0605 *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah: a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;	Pentadbir Sistem; Pentadbir Pangkalan Data

b) Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat Rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian perlu dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: a) Semua tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;	PSU (KnR); BTM SUK Selangor

c) Semua peralatan mestilah melalui proses UAT semasa pemasangan dan konfigurasi;

d) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

e) Semua capaian kepada Internet dan sistem aplikasi mestilah melalui *firewall* dan diselia oleh PSU (KnR);

f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PEJABAT SUK SELANGOR;

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

h) Memasang perisian IPS bagi mengesan dan menghalang sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PEJABAT SUK SELANGOR,

i) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j) Semua pengguna hanya dibenarkan menggunakan rangkaian PEJABAT SUK SELANGOR kecuali mendapat kebenaran dari Bahagian Teknologi Maklumat PEJABAT SUK SELANGOR dan penggunaan *modem* adalah dilarang sama sekali;

k) Sebarang penyambungan rangkaian yang bukan di bawah kawalan PEJABAT SUK SELANGOR adalah tidak dibenarkan; dan

l) Kemudahan bagi *Wireless* LAN perlu dipastikan kawalan keselamatan.

0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Media Mudah Alih	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada SUB (BTM) / pemilik sistem terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media	
Di antara prosedur-prosedur pengendalian media yang perlu dipatuhi termasuk: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; dan f) Media yang mengandungi maklumat terperingkat hendaklah dihapus atau dimusnahkan mengikut peraturan dan prosedur yang betul dan selamat.	Pentadbir Sistem; Pengguna

060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua
0608 Pengurusan Pertukaran Maklumat **Objektif:** Memastikan keselamatan pertukaran maklumat dan perisian antara PEJABAT SUK SELANGOR/agensi dan mana-mana entiti luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara PEJABAT SUK SELANGOR dengan pihak luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PEJABAT SUK SELANGOR; dan d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya;	SUB (TM); ICTSO; Pentadbir Sistem

060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di PEJABAT SUK SELANGOR hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; "Garis Panduan Penggunaan Mel Elektronik Pejabat SUK Selangor" dan mana-mana undang-undang bertulis yang berkuat kuasa. Di antara prosedur-prosedur pengurusan e-mel termasuk: a) Akaun atau alamat e-mel yang diperuntukkan oleh PEJABAT SUK SELANGOR sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Permohonan E-mel hendaklah dibuat dengan melengkapkan Borang "Borang Pengurusan E-mel" yang boleh diperolehi dari Portal Selangor atau Bahagian Teknologi Maklumat, SUK SELANGOR; c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; e) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; f) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;	PSU (KnR); Semua

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

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

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

j) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com dan sebagainya) tidak boleh digunakan untuk tujuan rasmi;

k) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing;

l) Menghadkan jenis dan saiz fail lampiran bagi tujuan mengelakkan jangkitan virus dan serangan e-mel bombing;

m) Penghantaran dokumen rasmi hendaklah menggunakan e-mel rasmi jabatan sahaja dan pastikan alamat e-mel penerima adalah betul;

n) Penggunaan e-mel PEJABAT SUK SELANGOR bagi tujuan peribadi adalah tidak dibenarkan;

o) Pentadbir e-mel perlu menetapkan had minimum kuota *mailbox*;

p) Pembersihan e-mel hendaklah dibuat sekiranya *mailbox* didapati tidak aktif selama dua (2) bulan atau melebihi kuota dan had masa yang ditetapkan;

q) Penghantaran lampiran dalam *format/extension* " *.exe, *.bat " dan " *.com" tidak dibenarkan dan pengguna yang menerima fail berkenaan juga adalah dilarang untuk membuka e-mel tersebut kerana boleh mengakibatkan penyebaran virus;

r) Hanya kakitangan PEJABAT SUK SELANGOR sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi jabatan; s) Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; t) Pengguna adalah dilarang sama sekali menggunakan alamat e-mel rasmi selangor bagi pendaftaran dalam mana-mana web/kumpulan/forum yang tidak berkaitan dengan urusan kerja rasmi; dan u) Bahagian Sumber Manusia PEJABAT SUK SELANGOR perlu memaklumkan sebarang status pengguna (bertukar jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke PEJABAT SUK SELANGOR) di bahagian masing-masing bagi tujuan pengemaskinian e-mel yang terlibat; Perlanggaran kepada mana-mana peraturan boleh menyebabkan penggantungan akaun pengguna atau mana-mana tindakan tatatertib yang bersesuaian.	

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

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

060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet.	Pentadbir Sistem; Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:- a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
0610 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat.	

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat. b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	SUB (BTM); Pentadbir Sistem
0611 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061101 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisa perkara-perkara berikut:- a) Sebarang percubaan pencerobohan kepada sistem ICT PEJABAT SUK SELANGOR; b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*). Pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);	ICTSO

c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwith* rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran PSU (KnR); dan i) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	
061102 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:- a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;	Pentadbir Sistem

c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) Maklumat akitiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir Sistem yang berkaitan hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061103 Sistem Log	
Fungsi-fungsi sistem log adalah seperti berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem
061104 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;	Pentadbir Sistem

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

d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;

e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisa dan diambil tindakan sewajarnya; dan

f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam PEJABAT SUK SELANGOR atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.

BIDANG 07
KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan pemprosesan maklumat.	BTM PEJABAT SUK SELANGOR; SUB (BTM), ICTSO; dan PSU (KnR)

0702 Pengurusan Capaian Pengguna

Objektif:
Mengawal capaian pengguna ke atas aset ICT PEJABAT SUK SELANGOR.

070201 Akaun Pengguna

` Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, Pentadbir Sistem perlu mengambil langkah-langkah berikut:	PSU (KnR); Semua

a) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b) Akaun pengguna (*user id*) hendaklah unik dan mencerminkan identiti pengguna; c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika kaedah penggunaannya melanggar peraturan; d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang, dan e) Pentadbir Sistem boleh menggantung dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	
070202 Hak Capaian (*Privilege*)	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PEJABAT SUK SELANGOR seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Pentadbir Sistem; Pengguna

b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) dan perlu mengandungi gabungan huruf besar dan kecil; d) Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Disarankan membuat pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Disarankan had masa pengesahan adalah selama dua (2) minit dan selepas had itu, sesi ditamatkan; j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 *Clear Desk* dan *Clear Screen*	
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.	Semua

Clear Desk and *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian PEJABAT SUK SELANGOR, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaiannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO; PSU (KnR)

070302 Capaian Internet

`

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:-

Semua

a) Penggunaan internet di PEJABAT SUK SELANGOR hendaklah dipantau secara berterusan oleh PSU (KnR) bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PEJABAT SUK SELANGOR;

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

c) Penggunaan proksi (sekiranya ada) yang telah ditetapkan oleh PEJABAT SUK SELANGOR bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan;

d) Penggunaan teknologi yang bersesuaian untuk mengawal aktiviti *video conferencing, video streaming, chat, downloading* adalah digalakkan bagi menguruskan penggunaan jalur lebar (*broadband*) yang maksimum dan lebih berkesan;

e) Penggunaan Internet hanyalah untuk **kegunaan rasmi sahaja**. Ketua Jabatan berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;

f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh SUB (BTM)/ICTSO/pegawai yang diberi kuasa;

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

h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha Bahagian sebelum dimuat naik ke Internet;

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

j) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PEJABAT SUK SELANGOR;

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

l) Penggunaan *modem* untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

m) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut;-

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

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

0704 Kawalan Capaian Sistem Pengoperasian

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

070401 Capaian Sistem Pengoperasian

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

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

b) Merekodkan capaian yang berjaya dan gagal;

c) Membekalkan kemudahan untuk pengesahan; bagi sistem, kata laluan kunci digunakan. Kualiti kata kunci perlu mendapat pengesahan; dan

d) Menghadkan masa penggunaan rangkaian bagi pengguna.

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan;

b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user;

c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan

d) Menyediakan tempoh penggunaan mengikut kesesuaian.

Perkara-perkara yang perlu dipatuhi termasuk berikut:

a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

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

e) Menghadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan

f) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	
070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Capaian sistem dan aplikasi di PEJABAT SUK SELANGOR adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian, keselamatan dan sensitiviti maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan	Pentadbir Sistem; Semua

f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibolehkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
0706 Peralatan Mudah Alih dan Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan jarak jauh	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut:- a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	SUB (BTM); ICTSO; Pemilik Sistem; Pentadbir Sistem

080102 Pengesahan Data *Input* dan *output*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan	Pentadbir Sistem

b) Data *Output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	
080103 Kawalan Prosesan	
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem
0802 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pentadbir Sistem; PSU (KnR)
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pentadbir Sistem; PSU (KnR)
080203 Penggunaan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem; PSU (KnR)
0803 Keselamatan Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	

080301 Kawalan Fail Sistem	
Fail sistem perlu dikawal dan dikendalikan dengan baik dan selamat. a) Proses pengemas kini fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b) Kod atau aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan Sistem	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal;	Pentadbir Sistem

c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh pemilik sistem. *Source code* adalah menjadi hak milik PEJABAT SUK SELANGOR.	BTM PEJABAT SUK SELANGOR dan Pentadbir Sistem
0805 Kawalan Teknikal Keterdedahan (*vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Maklumat mengenai ancaman teknikal sistem maklumat yang digunakan perlu diperolehi. Pendedahan organisasi kepada ancaman teknikal perlu dinilai bagi mengenalpasti tahap risiko yang bakal dihadapi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	ICTSO; Pentadbir Sistem

BIDANG 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

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

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CERT SELANGOR dengan kadar segera dan semua maklumat adalah dianggap SULIT: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di PEJABAT SUK SELANGOR sepertimana di **LAMPIRAN 2.**	ICTSO; SELANGOR CERT; Pengguna

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

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

i) **Pelaporan**

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada Jawatankuasa CERT SELANGOR untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah **SULIT,** dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.

ii) **Tanggungjawab Jawatankuasa CERT SELANGOR**

Jawatankuasa CERT SELANGOR akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya.

iii) **Tanggungjawab Pengguna**

Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.

iv) **Tindakan Dalam Keadaan Berisiko Tinggi**

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.

0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat Insiden Keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisa bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada PEJABAT SUK SELANGOR. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO, CERT SELANGOR

BIDANG 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif :

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

100101 Pelan Pengurusan Kesinambungan Perkhidmatan

Pelan Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management* – BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian: i) Mengenal pasti semua tanggungjawab dan prosedur kecemasan dan pemulihan; ii) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; iii) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; iv) Mendokumentasikan proses dan prosedur yang telah dipersetujui; v) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; vi) Membuat *backup*; dan vii) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	CIO; SUB (BTM)

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

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

b) Senarai personnel PEJABAT SUK SELANGOR dan pembekal beserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;

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

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

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

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

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

PEJABAT SUK SELANGOR hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

BIDANG 11
PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif

Meningkatkan tahap keselamatan ICT bagi mengelak daripada perlanggaran kepada DKICT PEJABAT SUK SELANGOR.

110101 Pematuhan Dasar

Setiap pengguna di PEJABAT SUK SELANGOR hendaklah membaca, memahami dan mematuhi DKICT PEJABAT SUK SELANGOR dan undang-undang atau peraturan-peraturan lain yang berkaitan. Semua aset ICT di PEJABAT SUK SELANGOR termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua

110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

110103 Pematuhan Keperluan Audit

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

110104 Keperluan Perundangan	
Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PEJABAT SUK SELANGOR adalah seperti di **Lampiran 3.**	Pengguna
110105 Pelanggaran Perundangan	
Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan. SUB (BTM) atau ICTSO adalah berhak untuk mengambil tindakan sebagaimana berikut:- i) Membuat teguran pertama melalui e-mel, sistem pemantauan atau mana-mana medium komunikasi secara atas talian; ii) ICTSO akan memberi e-mel/surat teguran kepada pesalah dan satu salinan emel akan turut diberi kepada Ketua Jabatan/pegawai pesalah; iii) Pesalah hendaklah memberi surat tunjuk sebab dalam tempoh tiga (3) hari bekerja dari tarikh e-mel/surat diterima; dan iv) SUB (BTM) atau ICTSO berhak mengambil tindakan berupa menarik balik kemudahan capaian internet/ peralatan ICT/ komputer (sementara/kekal) bergantung kepada jenis dan tahap kesalahan.	Pengguna

Glosari	
Antivirus	Perisian yang mengimbas virus pada peralatan ICT seperti komputer, *server* serta media storan, seperti cakera keras (*hard disk*) dan disket (*diskette*) untuk sebarang kemungkinan adanya virus.
Aset ICT	Terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (Cth: di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
BRP	*Business Resumption Planning* Pelan Kesinambungan Perkhidmatan
BTM	Bahagian Teknologi Maklumat (*Information Technology Department*).
CCTV	*Closed-circuit television system* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CIA[3]	*Confidentiality, Integrity, Authenticity, Accessibility, Accountability.*
CERT Agensi	*Computer Emergency Response Team* Organisasi yang ditubuhkan untuk Membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat bagi menyokong arahtuju sesebuah organisasi.
Data center	Pusat simpanan data.

Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
E-mel	Mel Elektronik (*Electronic Mail*).
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Juga pemisah di antara rangkaian luar dan dalam. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft*/*espionage*), penipuan(*hoaxes*).
GCERT	*Government Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology.*
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan ICT di sesebuah organisasi.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
IDS	*Intrusion Detection System* (Sistem Pengesan Pencerobohan) Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
IPS	*Intrusion Prevention System* (Sistem Pencegah Pencerobohan) Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau *malicious code*. E.g. *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Jurutera tempatan (KP)	Jurutera Tempatan (Khidmat Pengurusan)
Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
KnR	Keselamatan dan Rangkaian
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.

Ligthning arrestor	Alat yang digunakan untuk mencegah daripada ancaman kilat.
Lock	Mengunci komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse*, *worm, spyware* dan sebagainya.
MODEM	*MOdulator DEModulator* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
NOC	*Network Operation Centre.*
Outsource	Maklumat yang diproses dan diperolehi di luar daripada sesuatu organisasi atau struktur kerja.
Pegawai Aset ICT	Pegawai yang telah diberi kuasa untuk mentadbir Aset ICT PEJABAT SUK SELANGOR iaitu PPTM Kanan (BTM).
PEJABAT SUK SELANGOR	Jabatan/Agensi yang akan menggunapakai dan tertakluk kepada DKICT PEJABAT SUK SELANGOR iaitu:- i) Pentadbiran SUK Selangor; dan ii) Pejabat Daerah/Tanah Negeri Selangor.
Pengguna	Semua individu yang menggunakan perkhidmatan/aplikasi/kemudahan ICT yang disediakan oleh PEJABAT SUK SELANGOR.
Pentadbir Pangkalan Data	Pegawai yang telah diberi kuasa mentadbir pangkalan data PEJABAT SUK SELANGOR yang terdiri daripada PSU/PPTM.
Pentadbir Rangkaian	Pegawai yang telah diberi kuasa mentadbir rangkaian PEJABAT SUK SELANGOR yang terdiri daripada PSU/ PPTM.

Pentadbir Sistem	Pegawai yang telah diberi kuasa mentadbir sesuatu sistem PEJABAT SUK SELANGOR yang terdiri daripada PSU/PPTM Kanan/PPTM.
Pentadbir Web	Pegawai yang telah diberi kuasa mentadbir semua Web rasmi PEJABAT SUK SELANGOR yang terdiri daripada PSU/PPTM.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pihak Ketiga	Pihak pembekal, perunding atau mana-mana pihak luar yang berurusan dengan PEJABAT SUK SELANGOR.
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam.
PSU	Penolong Setiausaha Gelaran bagi jawatan Pegawai Teknologi Maklumat di PEJABAT SUK SELANGOR.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.

Server	Pelayan
SUB (BTM)	Setiausaha Bahagian, Bahagian Teknologi Maklumat
SUB (BKP)	Setiausaha Bahagian, Bahagian Khidmat Pengurusan
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian CSMA/CD secara mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
UAT	*User Acceptance Test*
UPS	*Uninterruptible Power Supply* Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video conference	Sidang Video. Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.

Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
Worms	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT PEJABAT SUK 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 PEJABAT SUK SELANGOR; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan Setiausaha Bahagian, Bahagian Teknologi Maklumat

.....

(Setiausaha Bahagian, Bahagian Teknologi Maklumat)

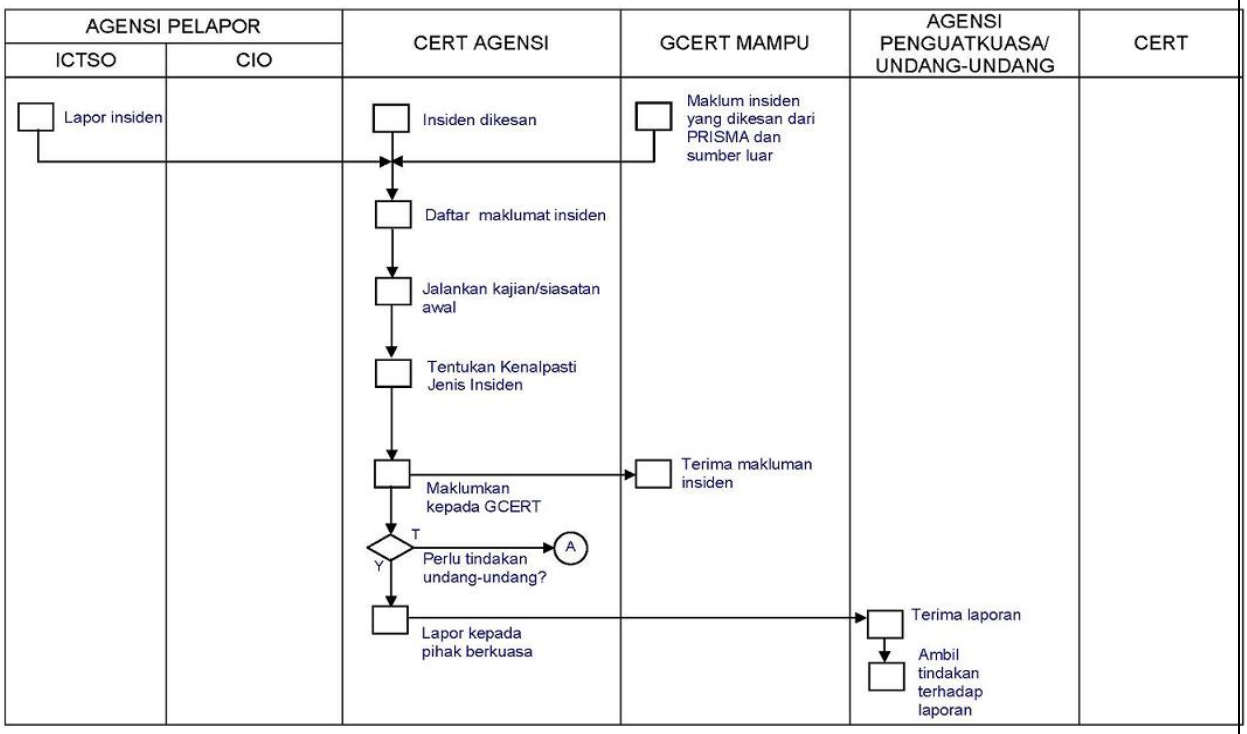
b.p. Setiausaha Kerajaan Negeri Selangor

Tarikh :

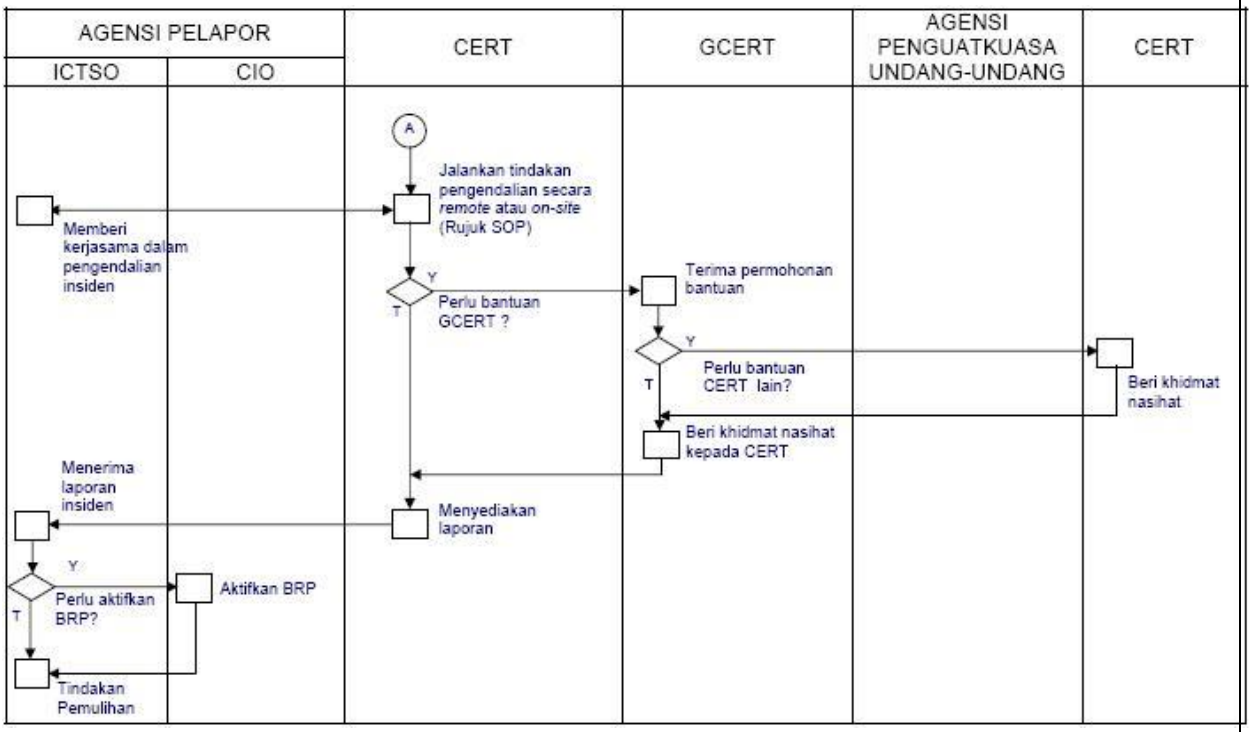
.....

Lampiran 2

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PEJABAT SUK SELANGOR



Rajah 2: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PEJABAT SUK SELANGOR



Lampiran 3

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 Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam,
g. Akta Tandatangan Digital 1997,
h. SPA Bil. 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 PenerimaanTender”,
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, dan
v. Pelan Kesinambungan Perkhidmatan.
w. Garis Panduan Penggunaan Mel Elektronik Pejabat SUK Selangor



GARIS PANDUAN
TATACARA PENGGUNAAN BAGI CAPAIAN INTERNET, INTRANET, E-MEL DAN *BROADBAND* TANPA WAYAR BAGI TUJUAN PENGURUSAN DAN PENTADBIRAN

BAHAGIAN TEKNOLOGI MAKLUMAT, PEJABAT SETIAUSAHA KERAJAAN NEGERI SELANGOR

1. TUJUAN

1.1. Kertas ini bertujuan untuk menyediakan satu garis panduan berkaitan tatacara penggunaan bagi capaian internet, e-mel rasmi dan *broadband* tanpa wayar (*Wireless Broadband*) bagi kakitangan di Pejabat Setiausaha Kerajaan (SUK) dan Sembilan (9) Pejabat Tanah/Daerah Negeri Selangor.

2. DEFINISI

2.1. Internet adalah infrastruktur saluran global atau rangkaian kerja global komputer dan merupakan punca maklumat yang sukar dikawal;

2.2. Intranet adalah jaringan komputer yang khusus untuk penggunaan pada lingkungan di dalam batasan suatu Organisasi atau Agensi. Dilihat dari sudut teknikalnya, Intranet didefinisikan sebagai penggunaan teknologi Internet dan WWW (World Wide Web) di dalam sebuah rangkaian komputer setempat (LAN). LAN adalah sekumpulan komputer-komputer yang saling dihubungkan pada suatu daerah atau lokasi tertentu. Intranet memaksimakan penggunaan LAN tersebut dengan menambah kemampuan-kemampuan Internet kedalamnya;

2.3. Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. Aplikasi e-mel ini digunakan secara meluas dan membenarkan komunikasi lebih daripada dua hala dengan cara yang pantas dan lebih sesuai untuk penulisan yang ringkas; dan

2.4. *Broadband* Tanpa Wayar adalah teknologi yang menyediakan rangkaian data dan internet tanpa wayar berkelajuan tinggi yang boleh dicapai melalui modem mudah alih, telefon atau peralatan yang lain.

3. LATARBELAKANG

3.1. Perkembangan teknologi maklumat dan komunikasi (ICT) telah membolehkan maklumat dihantar dan diterima dengan pantas. Kemudahan ini telah menyumbangkan kepada penggunaan Internet, e-mel dan *broadband* tanpa wayar secara meluas dalam menyokong pelaksanaan tugas harian dalam perkhidmatan awam;

3.2. Sehubungan itu, satu garis panduan mengenai tatacara pengunaan yang jelas perlu diwujudkan bagi menyokong kepada penggunaan kemudahan-kemudahan ini secara berkesan di Pejabat SUK dan Pejabat Tanah/Daerah Negeri Selangor;

3.3. Garis Panduan ini adalah tambahan kepada Dasar Keselamatan ICT yang lebih menekankan kepada tatacara penggunaan capaian internet, intranet, e-mel dan *broadband* tanpa wayar ini supaya diterima pakai untuk kegunaan pegawai dan kakitangan bagi tujuan pengurusan dan pentadbiran di Pejabat SUK dan Pejabat Tanah/Daerah Negeri Selangor; dan

3.4. Dalam menyediakan garis panduan ini, rujukan juga telah dibuat kepada dokumen-dokumen rasmi yang berikut:

3.4.1. *Malaysia Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) bertarikh 15 Januari 2002;

3.4.2. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bil.1 Tahun 2003, Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik Di Agensi-agensi Kerajaan bertarikh 28 November 2003;

3.4.3. Surat Arahan Ketua Pengarah MAMPU, Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan bertarikh 1 Jun 2007; dan

3.4.4. Dasar Keselamatan ICT (Pejabat SUK Negeri Selangor)

4. KUASA CAPAIAN

4.1. BTM berhak untuk membuat capaian jarak jauh terhadap aset ICT Pejabat SUK Negeri Selangor sekiranya mendapat kebenaran dari Setiausaha Bahagian atau ICTSO atau Ketua Bahagian pengguna aset atau pengguna aset sendiri.

5. SEBAB-SEBAB KAWALAN PENGAGIHAN DAN PENGGUNAAN DIPERLUKAN

5.1. Capaian dan penggunaan internet yang tidak terkawal boleh:-

5.1.1. Menyebabkan kesesakan laluan dan gangguan keapda aplikasi-aplikas rasmi Kerajaan;

5.1.2. Menyebabkan produktiviti oraganisasi dan kakitangan menurun akibat masa yang panjang diperuntukkan semasa melayari Internet;

5.1.3. Merosakkan Imej Agensi dan Perkhidmatan Awam dengan melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti dinyatakan dalam PKPA Bil.1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik Di Agensi-agensi Kerajaan bertarikh 28 November 2003; dan

5.1.4. Ancaman kepada keselamatan maklumat dan peralatan ICT organisasi kerana capaian kepada laman-laman di Internet yang boleh mendedahkan kepada ancaman siber.

5.2. Capaian dan penggunaan e-mel yang tidak terkawal boleh:-

5.2.1. Penggunaan e-mel rasmi tanpa kawalan boleh mendedahkan maklumat rasmi jabatan; dan

5.2.2. Merosakkan Imej Agensi dan Perkhidmatan Awam dengan melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel rasmi kerajaan seperti di nyatakan dalam PKPA Bil.1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik Di Agensi-agensi Kerajaan bertarikh 28 November 2003.

5.3. Capaian dan penggunaan *Broadband* Tanpa Wayar yang tidak terkawal boleh:-

5.3.1. Penggunaan *Broadband* tanpa wayar yang dibuat tanpa kawalan akan memberi kesan kepada prestasi dan mutu kerja kakitangan; dan

5.3.2. Ancaman kepada keselamatan dan kesahihan maklumat kerana pengguna terdedah kepada ancaman serangan siber.

6. TATACARA PENGGUNAAN

6.1. Tatacara penggunaan internet, e-mel dan broadband tanpa wayar adalah:

6.1.1. Tertakluk kepada Pekeliling Kemajuan Perkhidmatan Awam Bilangan 1 Tahun 2003 – "**Garis Panduan Mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi-agensi Kerajaan bertarikh 28 November 2003"**.

6.2. Selain dari itu, pengguna adalah tertakluk kepada:

6.2.1. Penggunaan e-mel:

6.2.1.1. Warga SUK Selangor perlu membuat permohonan untuk mendapatkan kemudahan e-mel bagi tujuan urusan rasmi melalui Borang Pengurusan E-mel yang boleh diperolehi dari laman web http://www.selangor.gov.my;

6.2.1.2. Kemudahan akaun e-mel akan diberikan kepada semua pegawai/kakitangan Gred 17 dan ke atas. Lain-lain kakitangan adalah tertakluk kepada kelulusan SUB (BTM) mengikut keperluan tugasan rasmi harian;

6.2.1.3. Akaun e-mel bukanlah hak mutlak individu;

6.2.1.4. Akaun atau alamat e-mel yang diperuntukkan hendaklah digunakan untuk tujuan rasmi. Sebarang penggunaan akaun e-mel milik orang lain adalah dilarang;

6.2.1.5. Pengguna adalah dilarang mendedahkan akaun dan kata laluan (*password*) kepada individu lain;

6.2.1.6. Pengguna dikehendaki menukarkan katalaluan sementara yang diberikan oleh Pentadbir E-mel kepada katalaluan persendirian. Minimum katalaluan ini adalah 8 aksara, yang terdiri daripada gabungan huruf, nombor dan

simbol;

6.2.1.7. Keselamatan katalaluan yang digunakan merupakan tanggungjawab sepenuhnya pengguna berkenaan. Andainya diragui yang katalaluan telah diketahui oleh orang lain, pengguna tersebut perlu menukarkan katalaluan dengan serta merta. Katalaluan sebaik-baiknya adalah gabungan abjad dan nombor;

6.2.1.8. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pengguna mestilah memastikan alamat e-mel penerima adalah betul;

6.2.1.9. Menggunakan e-mel bukan untuk tujuan lain seperti menyedia dan menghantar maklumat berulang-ulang yang berupa gangguan, menyedia, memuat naik, memuat turun dan menyimpan maklumat yang mengandungi unsur-unsur lucah atau sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan, atau menggunakan e-mel untuk tujuan komersial, politik, perjudian dan sebagainya;

6.2.1.10. Pengguna e-mel dikehendaki menggunakan kemudahan ini dengan penuh bertanggungjawab dan mengamalkan etika penggunaan e-mel bagi menjamin keselesaan pengguna-pengguna lain;

6.2.1.11. Pengguna e-mel adalah dilarang menggunakan apa cara sekalipun untuk menyamar sebagai penghantar e-mel yang sah;

6.2.1.12. Pengguna e-mel adalah dilarang untuk melibatkan diri dalam penghantaran mel sampah (flaming), mel bom (mail bombing) dan mel spam. Mel sampah adalah mel yang tidak berkaitan yang dihantar kepada seseorang dan mel bom adalah mel penghantaran mel secara bertalu-talu (looping) yang menyebabkan penerima mengalami masalah. Mel spam adalah mel yang dihantar oleh penghantar yang tidak diketahui seperti menerima mel daripada seorang jurujual yang cuba menjual produknya melalui e-mel;

6.2.1.13. Pengguna e-mel juga dilarang untuk mendaftar diri dalam senarai mel tertentu (contoh: yahoo.groups, google.groups) yang menyebabkan penerimaan e-mel dalam jumlah yang banyak pada setiap hari yang mana anda sendiri tidak berupaya membacanya. Sila gunakan kemudahan e-mel percuma lain untuk mendaftar dan menggunakan kemudahan ini;

6.2.1.14. Pengguna juga dikehendaki 'unsubscribe' sebarang e-mel yang tidak dikehendaki yang telah di 'subscribe' walaupun mungkin telah dilakukan oleh orang lain;

6.2.1.15. Penghantaran e-mel ke alamat group G_SUK_user adalah dilarang kecuali dengan kebenaran Pentadbir e-mel;

6.2.1.16. Pengguna e-mel perlu memastikan fail yang dihantar melalui lampiran (*attachment*) bebas dari virus dan hendaklah sentiasa mengimbas fail dalam kotak mel (*mailbox*);

6.2.1.17. Pengguna atau Ketua Bahagian bertanggungjawab bagi memaklumkan kepada pentadbir e-mel sekiranya bercuti panjang atau berkursus panjang atau bertukar keluar, melepaskan jabatan, berhenti atau bersara. Akaun e-mel yang didapati tidak digunakan atau tidak aktif lebih daripada 90 hari secara berterusan tanpa sebab yang munasabah akan dihapuskan bagi mengelakkan salahguna e-mel pada masa akan datang;

6.2.1.18. Jangan menghantar salinan mesej kepada orang lain yang tidak memerlukannya terutama kepada kumpulan e-mel jabatan (email groups). Ini akan membebankan sistem e-mel terutama sekiranya mesej mempunyai lampiran yang banyak dan bersaiz besar;

6.2.1.19. Jangan melampirkan fail melainkan ianya benar-benar diperlukan. Semua lampiran menggunakan format .zip, .exe, .com, .bat, .scr, .vbs, .js dan .shs tidak dibenarkan kerana format ini akan memudahkan penyebaran virus. Pengguna dinasihatkan tidak sekali-kali menjalankan (dengan mengklik) fail yang mempunyai format lampiran tersebut;

6.2.1.20. Pengguna hendaklah memastikan program Anti-Virus telah dipasang pada komputer dengan data virus yang terkini untuk membolehkan sebarang fail yang mengandungi virus dikesan di komputer pengguna semasa fail e-mel diterima;

6.2.1.21. Peraturan asas bagi penggunaan e-mel yang baik:

1. Setiap pegawai adalah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing;

2. Jangan membiarkan mesej bertambah di dalam *folder inbox*. Pengguna

mungkin terlepas pandang mesej yang lebih utama yang tersorok di antara yang lama ataupun mesej-mesej yang sudahpun dibaca;

3. Sebaiknya buatlah *folder* berasingan yang khusus dan bersesuaian serta memindahkan mesej-mesej tersebut ke *folder* berkenaan untuk rujukan di masa depan;

4. Memadamkan mesej yang tidak berkaitan sebaik sahaja menerimanya terutamanya spam dan e-mel bervirus. Sila laporkan dengan kadar segera kepada Pentadbir e-mel sekiranya terdapat spam atau e-mel bervirus; dan

5. Membuka *folder Sent Items* sekurang-kurangnya sekali seminggu dan memadamkan salinan mesej-mesej lama yang telah berjaya dikirim sekiranya tidak lagi diperlukan.

6.2.1.22. Keselamatan e-mel:

1. Simpan salinan mesej yang penting terutamanya lampiran;

2. Jangan menghantar e-mel kepada seseorang dengan mengunakan akaun penguna dan katalaluan orang lain melalui apa cara sekalipun;

3. Pengguna hendaklah sentiasa mengimbas fail dalam kotak mel (*mailbox*) dengan perisian antivirus. Berwaspadalah kerana e-mel adalah cara paling mudah untuk menghantar virus dari sebuah komputer ke komputer yang lain. Pengguna juga hendaklah memastikan fail yang akan dihantar melalui lampiran (*attachment*) bebas dari virus. Jika tidak, dengan cara tidak sengaja mungkin telah menyebabkan virus itu merebak dengan meluas dan merumitkan langkah-langkah pembaikan; dan

4. Jangan menggunakan e-mel rasmi jabatan dengan mendaftar dalam senarai e-mel, kumpulan perbincangan, muat turun, pendaftaran di internet yang menyebabkan pengguna menerima sejumlah e-mel berbentuk komersil, porno dan lain-lain yang tidak diundang dengan banyak pada setiap hari (e-mel spam).

6.2.1.23. Perkara-perkara lain yang perlu diambilkira bagi kandungan e-mel yang dihantar:

1. Ringkaskan mesej e-mel seberapa yang boleh;

2. Elakkan menggunakan e-mel untuk perkara-perkara yang tidak penting seperti gossip dan sebagainya;

3. Gunakan bahasa yang berhemah tinggi dan sesuai dengan penerima e-mel terutamanya bagi e-mel yang dihantar kepada lebih dari seorang penerima;

4. Tidak mem'forward'kan sebarang e-mel yang bersifat persendirian kepada orang lain terutama kepada e-mel kumpulan; dan

5. Pengirim e-mel harus sentiasa mencatat Perkara E-mel (*Subject*) dengan sempurna bagi membantu penerima e-mel membezakan e-mel sebenar dan yang palsu.

6.2.1.24. Tidak mematuhi mana-mana peraturan yang ditetapkan boleh mengakibatkan kemudahan ini ditarik balik dan/atau dikenakan tindakan;dan

6.2.1.25. Sebarang permasalahan penggunaan e-mel rasmi hendaklah dilaporkan kepada Pentadbir E-mel bagi memudahkan kerja-kerja penyelenggaraan dilakukan.

6.2.2.Penggunaan internet:

6.2.2.1. Penggunaan e-mel yang bukan rasmi (seperti @yahoo atau @gmail) dan yang rasmi serta penggunaan media internet dan media jaringan sosial seperti blog dan facebook:

1. Dengan bertujuan menjejaskan perkhidmatan awam dan kedaulatan Negara adalah dilarang sama sekali; dan

2. Tidak melibatkan penyebaran maklumat dan dokumen terperingkat. Semua maklumat Kerajaan hendaklah dikendalikan mengikut prosedur dan peraturan yang telah ditetapkan. Sebarang perbuatan mendedahkan maklumat jabatan adalah bertentangan dengan Pekeliling Am.

6.2.3.Penggunaan *broadband* tanpa wayar:

6.2.3.1. Penyambungan *broadband* tanpa wayar kepada aset ICT Pejabat SUK Selangor adalah dilarang sama sekali kecuali melalui penggunaan *broadband* tanpa wayar yang dibekalkan oleh BTM/jabatan dengan tujuan.

1. Membuat kerja rasmi di luar jabatan;

2. Memerlukan membuat pengujian akses terhadap aplikasi / rangkaian; dan

3. Keperluan mendesak yang mendapat kebenaran Ketua Bahagian.