DASAR KESELAMATAN MAKLUMAT

LEMBAGA TABUNG ANGKATAN TENTERA (LTAT)

VERSI 3.0
2019

ISI KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan Maklumat LTAT diwujudkan untuk menjamin kesinambungan urusan LTAT dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT LTAT ialah seperti berikut:

a. Memastikan kelancaran operasi LTAT dan meminimumkan kerosakan atau kemusnahan.

b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.

c. Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

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

Keselamatan maklumat ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

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

b. Menjamin setiap maklumat adalah tepat dan sempurna.

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.

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

Dasar Keselamatan Maklumat LTAT merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

b. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan.

c. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya.

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

Selain dari itu, langkah-langkah ke arah menjamin keselamatan maklumat 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 LTAT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan Maklumat LTAT menetapkan keperluan-keperluan asas berikut:

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

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

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan Maklumat LTAT ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan LTAT. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya.

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada LTAT;

c. 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 pejabat seperti sistem Biodoor.

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

d. Data atau Maklumat

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

e. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian LTAT bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f. Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a)** - **(e)** 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 Dasar Keselamatan Maklumat LTAT dan perlu dipatuhi adalah seperti berikut:

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna

memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15.

b. Hak akses minimum

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

c. Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan.

ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa.

iii. Menentukan maklumat sedia untuk digunakan.

iv. Menjaga kerahsiaan kata laluan.

v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan.

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

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

d. Pengasingan

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

e. Pengauditan

Pengauditan adalah tindakan untuk mengenalpasti insiden berkaitan keselamatan atau mengenalpasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.
Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian

hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f. Pematuhan

Dasar Keselamatan Maklumat LTAT hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g. Pemulihan

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

h. Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

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

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

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

a. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian.

b. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh Jawatankuasa Pengurusan Risiko.

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

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

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan Maklumat	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan LTAT dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Eksekutif (KE)/ Wakil Pengurusan (WP) LTAT selaku Pengerusi Jawatankuasa Keselamatan ICT (JKICT) LTAT. JKICT ini terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan.	**KETUA EKSEKUTIF / WAKIL PENGURUSAN LTAT**
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna LTAT (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	**ICTSO**
010103 Penyelenggaraan Dasar	
Dasar Keselamatan Maklumat LTAT adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan Maklumat LTAT: a. Kenalpasti dan tentukan perubahan yang diperlukan. b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), LTAT. c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT. d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	**ICTSO**
010104 Pengecualian Dasar	
Dasar Keselamatan Maklumat LTAT adalah terpakai kepada semua pengguna ICT LTAT dan tiada pengecualian diberikan.	**Semua**

PERKARA 02
ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan Maklumat LTAT.

020101 Ketua Eksekutif (KE) / Wakil Pengurusan (WP) LTAT

Ketua Eksekutif adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan Maklumat LTAT. b. Memastikan semua pengguna mematuhi Dasar Keselamatan Maklumat LTAT. c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi. d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan Maklumat LTAT. e. Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), LTAT.	**KE / WP LTAT**

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi LTAT ialah Penolong Pengurus Besar (JPTM) Peranan dan tanggungjawab CIO adalah seperti berikut: a. Membantu KE dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT. b. Menentukan keperluan keselamatan ICT. c. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT LTAT.	**CIO**

020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi LTAT ialah Pengurus JPTM atau Penolong Pengurus atau Eksekutif Kanan Teknologi Maklumat. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT LTAT. b. Menguatkuasakan pelaksanaan Dasar Keselamatan Maklumat LTAT. c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan Maklumat LTAT kepada semua pengguna. d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan Maklumat LTAT. e. Menjalankan pengurusan risiko. f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan LTAT berdasarkan hasil penemuan dan menyediakan laporan mengenainya. g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. h. Melaporkan insiden keselamatan ICT kepada CIO dan Pengurusan, LTAT. i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera. j. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. k. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	**ICTSO**
020104 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT LTAT. b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya. c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat.	**Pengguna**

d. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT LTAT dan menjaga kerahsiaan maklumat LTAT. e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. f. Menghadiri program-program kesedaran mengenai keselamatan ICT. g. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan Maklumat LTAT sebagaimana **Lampiran 1**.	
020105 JawatanKuasa Keselamatan ICT LTAT	
Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT LTAT. Keanggotaan JKICT LTAT adalah seperti berikut: Pengerusi : Ketua Eksekutif (KE) Ahli : 1. Ketua Pegawai Maklumat (CIO) 2. Ketua-ketua Jabatan 3. Pegawai Keselamatan ICT (ICTSO) Urus Setia bagi JKICT LTAT ialah urus setia yang mengendalikan Mesyuarat Kajian Semula ISMS (MKS ISMS). Bidang kuasa: a. Memperakukan/meluluskan dokumen Dasar Kesemalatan Maklumat (DKM) LTAT. b. Memantau tahap pematuhan keselamatan ICT. c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam LTAT yang mematuhi keperluan DKM LTAT. d. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT. e. Memastikan DKICT LTAT selaras dengan dasar-dasar ICT kerajaan semasa. f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa. g. Membincang tindakan yang melibatkan pelanggaran DKICT LTAT. h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	**JKICT LTAT**

020106 Pasukan Tindak Balas Insiden Keselamatan ICT LTAT (LCERT)	
Keanggotaan LCERT adalah seperti berikut: <u>Pengurus</u> Ketua Pegawai Maklumat (CIO), LTAT. <u>Ahli</u> 1. Pegawai Keselamatan ICT (ICTSO), LTAT. 2. Juruanalisa Sistem. 3. Eksekutif Kanan Teknologi Maklumat. 4. Eksekutif Teknologi Maklumat. 5. Pengatur Rancangan Komputer. Peranan dan tanggungjawab LCERT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden. b. Merekod dan menjalankan siasatan awal insiden yang diterima. c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum. d. Menasihati LTAT mengambil tindakan pemulihan dan pengukuhan. e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada LTAT.	

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 termasuk yang berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan Maklumat LTAT.	**CIO,** **ICTSO, Pengurus ICT, Pentadbir Sistem**

b. Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian. c. Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga. d. Akses kepada aset ICT LTAT perlu berlandaskan kepada perjanjian kontrak. e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan Maklumat LTAT. ii. Tapisan Keselamatan. iii. Perakuan Akta Rahsia Rasmi 1972. iv. Hak Harta Intelek.	**dan** **Pihak Ketiga**

PERKARA 03
PENGURUSAN ASET

0301 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LTAT

030101 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikenalpasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini. b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di LTAT. d. Peraturan bagi pengendalian asset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan. e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT dibawah kawalannya.	**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 atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. 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. d. Terhad.	**Semua**

030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. c. Menentukan maklumat sedia untuk digunakan. d. Menjaga kerahsiaan kata laluan. e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	**Semua**

PERKARA 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

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

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan LTAT serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan. b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan LTAT serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**

040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan LTAT serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh LTAT. b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT LTAT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa. c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan LTAT serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh LTAT. 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	**Semua**

diperlukan, pengguna boleh merujuk kepada Jabatan Kewangan & Pentadbiran (JKP).	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua asset ICT dikembalikan kepada LTAT mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh LTAT dan/atau terma perkhidmatan.	**Semua**

PERKARA 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 dikenalpasti 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. Mengehadkan jalan keluar masuk. e. Mengadakan kaunter kawalan. f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat. g. Mewujudkan perkhidmatan kawalan keselamatan. h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini. 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. l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	**Semua**

050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawalan masuk untuk setiap tingkat di Bangunan LTAT dikawal oleh sistem Biodoor (jari atau kad pintar kakitangan) dan sistem CCTV.	**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. Kawasan larangan di LTAT adalah bilik fail, bilik server, rack switch dan bilik PABX. a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes - kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	**JKP**
0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT LTAT 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. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan. c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan. d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT. e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya. f. Pengguna mesti memastikan perisian antivirus pada computer peribadi mereka sentiasa aktif *(activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan.	**Semua**

g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan.

h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran.

i. Peralatan-peralatan kritikal perlu disokongoleh *Uninterruptable Power Supply* (UPS).

j. Semua peralatan ICT 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 rak khas.

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

l. Peralatan ICT yang hendak dibawa keluar dari premis LTAT, perlulah mendapat kelulusan JKP dan direkodkan bagi tujuan pemantauan.

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada JKP dengan segera.

n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa.

o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran JKP.

p. Sebarang kerosakan peralatan ICT hendaklah dirujuk pada prosedur *Incident Management* untuk dibaikpulih.

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

r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal.

s. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir *(administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT.

t. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja.

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

v. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.

050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, *usb drive,* CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja. c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan. d. Akses dan pergerakan media storan hendaklah direkodkan. 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. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat. h. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	**Semua**
050203 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan LTAT. b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Ketua Jabatan. c. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
050204 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti.	**JKP**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar. b. Memastikan perkakasan hanya boleh diselenggara oleh 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 pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. f. Semua penyelenggaraan mestilah mendapat kebenaran daripada JKP.	
050205 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis LTAT 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.	**Semua**
050206 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh LTAT dan ditempatkan di LTAT. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan LTAT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degaussing* atau pembakaran. b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan.	**Semua,** **Pegawai JKP** **dan** **Pegawai PTM LTAT**

c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.

d. Pegawai JKP hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya.

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

f. Pegawai JKP bertanggungjawab merekodkan butir—butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori SPA.

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

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

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalam CPU seperti RAM, *hardisk, motherboard* dan sebagainya.

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di LTAT.

iii. Memindah keluar dari LTAT mana-mana peralatan ICT yang hendak dilupuskan.

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab LTAT.

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

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT LTAT 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. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: 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 kawasan yang mempunyai kemudahanICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan. c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan. d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT. e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT. f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan computer. 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 Akses kepada saluran *riser* hendaklah sentiasa dikunci.	**Semua**
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana *(generator)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	**JKP & PPHM**

050303 Kabel	
Kabel komputer 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 *wiretapping.* d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	**JPTM & PPHM**
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan. b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Insiden LTAT.	**JKP**
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat LTAT dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar. b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan. c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan. d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara. e. Menggunakan enkripsi(*encryption)* ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	**Semua**

PERKARA 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:

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

060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, dikenalpasti dan digunapakai hendaklah didokumen, disimpan dan dikawal. b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output,* bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	**Semua**

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu. b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	**Semua**

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	**Semua**

tidak dibenarkan ke atas aset ICT. b. Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. c. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production.* Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	
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 perkhidmatandan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga. b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau dan disemak semula dari semasa ke semasa. c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	**Semua**
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.	**JPTM**

060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**JPTM**
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 dipatuhi adaIah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat. b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya. d. Mengemas kini anti virus dengan pattern antivirus yang terkini. e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya. h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	**Semua**
060402 Perlindungan dari Mobile Code	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	**Semua**

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* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat. c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. d. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	**Semua**

0606 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk. b. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja. c. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh JPTM. d. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JPTM.	**JPTM**

e. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO. f. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LTAT. g. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang. h. Sebarang penyambungan rangkaian yang bukan di bawah kawalan LTAT adalah tidak dibenarkan. i. Semua pengguna hanya dibenarkan menggunakan rangkaian LTAT sahaja dan penggunaan modem / *USB Broadband* adalah dilarang sama sekali. j. 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 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	**Semua**
060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitivity 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. f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	**Semua**

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. c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	**Semua**
0608 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara LTAT dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi. b. Perjanjian (Akta & Peraturan) perlu diwujudkan untuk pertukaran maklumat dan perisian di antara LTAT dengan agensi luar. c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari LTAT. d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi.	**Semua**
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di LTAT 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"* dan mana-mana undang-undang bertulis yang berkuatkuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh LTAT sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. b. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul.	**Semua**

c. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua puluh megabait (20Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan. d. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui. e. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel. f. Setiape-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan. g. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan. h. Penggunahendaklah 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 bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
060803 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. c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	**Semua**
0609 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
060901 Jejak Audit	

Setiap sistem mestilah mempunyai jejak audit *(audit trail).* Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi. b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. c. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya.	**Pentadbir Sistem ICT**
060902 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	**Pemilik Sistem**
060903 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala. c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan. d. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam LTAT atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	**Pemilik Sistem**

PERKARA 07 KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	
Objektif: Mengawal capaian ke atas maklumat.	
070101 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. la 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. Mengawal capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna. b. Mengawal capaian ke atas perkhidmatan rangkaian dalaman dan luaran. c. Mengawal keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih. d. Mengawal capaian ke atas kemudahan pemprosesan maklumat.	**LTAT & ICTSO**
0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT LTAT.	
070201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh LTAT sahaja boleh digunakan. b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identity pengguna. c. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LTAT. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan. d. Penggunaan akaun milik orang lain atau akaun yang dikongsi	**JKP**

bersama adalah dilarang. e. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja. ii. Bersara. iii. Ditamatkan perkhidmatan.	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	**JKP**
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 LTAT seperti berikut: a. Dalamapa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun. b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi. c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara angka dan symbol. d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun. e. Katalaluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama. f. Katalaluan hendaklah tidak dipaparkan semasa *input,* dalam laporan atau media lain dan tidak boleh dikodkan di dalam program. g. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula. h. Katalaluan hendaklah berlainan daripada pengenalan identiti pengguna. i. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian. j. Mengelakkan penggunaan semula kata laluan yang baru digunakan. Nota: Penggunaan katalaluan bagi kriteria di atas tidak tertakluk kepada	**Semua & Pentadbir Sistem ICT**

penggunaan kata laluan pada server IBM i-Series.	
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan computer. b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci. c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	**Semua**
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 *(interface*) yang bersesuaian di antara rangkaian LTAT, rangkaian agensi lain dan rangkaian awam. b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**JPTM**
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di LTAT hendaklah dipantau secara berterusan oleh JPTM 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 LTAT.	**Pengurus JPTM & Semua**

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

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

d. Penggunaan Internet hanyalah untuk kegunaanrasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya.

e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengurusan/ pegawai yang diberi kuasa.

f. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukansumber Internet hendaklah dinyatakan.

g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet.

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

i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh LTAT.

j. 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 Pengurusan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan.

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

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

   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: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan. b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan. b. Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user.* c. Menjana amaran *(alert)* sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin. b. Mewujudkan satu pengenalan diri (ID) yangunik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja. c. Menghadkan dan mengawal penggunaan program. d. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	**JPTM**
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 aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan	**Pentadbir Sistem**

maklumat yang telah ditentukan. b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log). c. Menghadkan capaian sistem dan aplikasi tertentu kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat. d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. e. Capaian sistem maklumat dan aplikasi melalui jarak jauh terhad kepada perkhidmatan dan kakitangan yang dibenarkan sahaja.	
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja 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. b. Pegawai dan kakitangan yang menggunakan peralatan mudah alih bertanggungjawab untuk memastikan keselamatan maklumat dan peralatan tersebut.	**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**

PERKARA 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 ketepatan maklumat. b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna. c. Aplikasi perlu mengandungi semakan pengesahan *(validation)* untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan. d. Semua system yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Pemilik Sistem**

080102 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian. b. Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	**Pemilik Sistem**

0802 Keselamatan Fail Sistem

Objektif:

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

080201 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut	**Pemilik Sistem dan Pentadbir Sistem ICT**

prosedur yang telah ditetapkan. b. Kod atau atur cara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji. c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian. d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal. e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
0803 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080301 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum 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 vendor. 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. e. Menghalang sebarang peluang untuk membocorkan maklumat.	**Pemilik Sistem dan Pentadbir Sistem ICT**
080302 Pembangunan Perisian Secara Outsource	
a. Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik system.	**Seksyen Teknologi Maklumat dan Pentadbir Sistem ICT**

0804 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080401 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas system pengoperasian dan system aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan. b. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi. c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**Pentadbir Sistem ICT**
0805 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080501 Enkripsi	
Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	**Semua**
080502 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	**Semua**
080503 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan terjejas sepanjang tempoh sah kunci tersebut. Sebarang perubahan perlu direkodkan bagi tujuan jaminan keselamatan dan jangka masa tempoh sah kunci tersebut.	**Semua**

PERKARA 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah *(adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. La mungkin suatu perbuatan yang melanggar Dasar Keselamatan Maklumat sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan Pengurusan dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa. b. Sistem maklumat digunakan tanpa kebenaranatau disyaki sedemikian. c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan. d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar. e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di LTAT sepertimana Prosedur SP-LTAT-20000 ICT-02.00.00 (Incident Management).	**Semua**

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

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

PERKARA 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

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

100101 Pelan Kesinambungan Perkhidmatan

Pelan Kesinambungan Perkhidmatan (Business Continuity Management - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Pengurusan. Perkara-perkara berikut perlu diberi perhatian: a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan. b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT. c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan. d. Mendokumentasikan proses dan prosedur yang telah dipersetujui. e. Membuat backup. f. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan. b. Senarai personel LTAT dan vendor berserta 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.	**JPRP**

d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia 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 apabila pelan dilaksanakan. LTAT hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

PERKARA 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan Maklumat LTAT.	
110101 Pematuhan Dasar	
Setiap pengguna di LTAT hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT LTAT dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di LTAT termasuk maklumat yang disimpan di dalamnya adalah hak milik LTAT. Ketua Jabatan/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT LTAT selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber LTAT.	**Semua**
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi 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	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di LTAT adalah seperti di **Lampiran 2.**	**Semua**
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan Maklumat LTAT boleh dikenakan tindakan tatatertib.	**Semua**

Tarikh Berkuatkuasa:

Dasar ini berkuatkuasa daripada tarikh pengeluarannya.

Puan Nik Amlizan Mohamed

Ketua Eksekutif
Lembaga Tabung Angkatan Tentera

Tarikh : 15/7/19

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN MAKLUMAT LTAT

Nama (Huruf Besar) : ……..…….....……

No. Kad Pengenalan : …….....…….....

Jawatan : …….....

Jabatan : .....…….....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Maklumat LTAT.

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
b/p : Ketua Eksekutif LTAT

Tarikh: .....

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Tabung Angkatan Tentera.
2. Peraturan Kewangan LTAT.
3. Peraturan Tata Tertib.
4. Arahan Keselamatan.
5. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.
6. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT).
7. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan.
8. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.
9. Akta Tandatangan Digital 1997.
10. Akta Rahsia Rasmi 1972.
11. Akta Jenayah Komputer 1997.
12. Akta Hak Cipta (Pindaan) Tahun 1997.
13. Akta Komunikasi dan Multimedia 1998.
14. Perintah-Perintah Am.
15. Arahan Perbendaharaan.
16. Arahan Teknologi Maklumat 2007.
17. Akta Perlindungan Data Peribadi 2010.