YAYASAN PAHANG

POLISI KESELAMATAN SIBER

YAYASAN PAHANG

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
18hb April 2017	2.1	YB Setiausaha Kerajaan Negeri Pahang Surat bertarikh 16hb Mei 2017 (SUK.PHG/PTM.007/7.016 Jld:5(15) telah dihantar kepada semua agensi di bawah pejabat SUK Negeri Pahang untuk diterima pakai dokumen Polisi Keselamatan Siber ver. 2.1 jika bersesuaian dan tertakluk kepada penerimaan oleh pihak berkuasa masing-masing	18hb April 2017
5hb Jun 2017	2.1	Pengurusan Tertinggi YP bil 8/2017 bersetuju untuk tindakan mengwujudkan Polisi Keselamatan Siber Yayasan Pahang dengan pindaaan yang bersesuaian dengan persekitaran Yayasan Pahang.	
17hb Julai 2017	2.1	Pengurusan Tertinggi YP bil 9/2017 bersetuju memperakukan pemakaian Polisi Keselamatan Siber Yayasan Pahang.	17hb Julai 2017

JADUAL PINDAAN POLISI KESELAMATAN SIBER
YAYASAN PAHANG

TARIKH	VERSI	BUTIRAN PINDAAN

KANDUNGAN MUKA SURAT

PENGENALAN

Polisi Keselamatan Siber Yayasan Pahang mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Polisi ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT bagi Yayasan Pahang.

OBJEKTIF

Polisi Keselamatan Siber Yayasan Pahang Pahang diwujudkan untuk menjamin kesinambungan urusan di dalam Yayasan Pahang dengan meminimumkan kesan insiden keselamatan ICT.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Pentadbiran Yayasan Pahang. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT Yayasan Pahang ialah seperti berikut:

(a) Memastikan kelancaran operasi bahagian-bahagian dan unit dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN POLISI

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

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

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) Melindungi maklumat rahsia rasmi 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; dan
d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Polisi Keselamatan Siber Yayasan Pahang 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 kemas kini. 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; dan
e) 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

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

1) Maklumat (contoh: fail, dokumen, data elektronik);
2) Perisian (contoh: aplikasi dan sistem perisian); dan
3) Fizikal (contoh: komputer, peralatan komunikasi dan media magnet).

Polisi ini adalah terpakai oleh semua pengguna di Yayasan Pahang termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Yayasan Pahang.

Aset ICT Yayasan Pahang terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan ICT Yayasan Pahang 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; dan

(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, Polisi Keselamatan Siber Yayasan Pahang 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 di Yayasan Pahang. 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 Yayasan Pahang;

(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 seperti sistem kad akses; dan

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 Yayasan Pahang. Contohnya, sistem dokumentasi, prosedur operasi, rekod- rekod Yayasan Pahang, 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 Yayasan Pahang bagi mencapai misi dan objektif. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(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 Polisi Keselamatan Siber Yayasan Pahang 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, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah 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 inidipatuhi, sistem ICT hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

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

d. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f. Pematuhan

Polisi Keselamatan Siber Yayasan Pahang 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

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

Yayasan Pahang 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 Yayasan Pahang 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.

Yayasan Pahang 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.

Yayasan Pahang perlu mengenal pasti 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 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 POLISI

0101 POLISI KESELAMATAN SIBER	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Yayasan Pahang dan perundangan yang berkaitan.	
010101 PELAKSANAAN POLISI	**TANGGUNGJAWAB**
Pelaksanaan Polisi ini akan dijalankan oleh Pengurus Besar Yayasan Pahang selaku Pengerusi Mesyuarat Jawatankuasan ICT Yayasan Pahang i) Pengurus Teknologi Maklumat (CIO) ii) Penolong Pengurus Teknologi Maklumat (ICTSO) iii) Pengurus Bahagian/Unit	Pengurus Besar Yayasan Pahang
010102 PENYEBARAN POLISI	**TANGGUNGJAWAB**
Polisi ini perlu disebarkan kepada semua pengguna di Yayasan Pahang yang menggunapakai (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	ICTSO
010103 PENYELENGGARAAN POLISI	**TANGGUNGJAWAB**
Polisi Keselamatan Siber ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Polisi Keselamatan Siber Yayasan Pahang : a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa ICT Yayasan Pahang/Pengurusan Tertinggi Yayasan Pahang; c. Maklum kepada semua pengguna perubahan yang telah dipersetujui; dan d. Polisi ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	ICTSO
010104 PENGECUALIAN POLISI	**TANGGUNGJAWAB**
Polisi Keselamatan Siber Yayasan Pahang adalah terpakai kepada semua pengguna ICT di Yayasan Pahang tanpa pengecualian.	Semua

BIDANG 02 ORGANISASI KESELAMATAN

0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber Yayasan Pahang.	
020101 SETIAUSAHA KERAJAAN NEGERI PAHANG	**TANGGUNGJAWAB**
Peranan dan tanggungjawab Pengurus Besar Yayasan Pahang adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Polisi Keselamatan Siber Yayasan Pahang; b. Memastikan semua pengguna mematuhi Polisi Keselamatan Siber Yayasan Pahang; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi Keselamatan Siber Yayasan Pahang.	Pengurus Besar
020102 KETUA PEGAWAI MAKLUMAT (CIO)	**TANGGUNGJAWAB**
Pengurus Teknologi Maklumat adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. Membantu Pengurus Besar Yayasan Pahang dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; dan c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Polisi Keselamatan Siber Yayasan Pahang serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT Yayasan Pahang.	CIO

020103 PEGAWAI KESELAMATAN ICT (ICTSO)	TANGGUNGJAWAB
Penolong Pengurus Teknologi Maklumat adalah merupakan ICTSO Yayasan Pahang. Peranan dan tanggungjawab ICTSO adalah seperti berikut : a. Memahami dan mematuhi Polisi Keselamatan Siber Yayasan Pahang; b. Menguatkuasakan Polisi Keselamatan Siber Yayasan Pahang; c. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Yayasan Pahang; d. Menentukan kawalan akses semua pengguna terhadap aset ICT Yayasan Pahang; e. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; f. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; g. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Yayasan Pahang; dan h. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan Siber Yayasan Pahang.	ICTSO
020104 PENTADBIR KESELAMATAN	**TANGGUNGJAWAB**
Penolong Pegawai Teknologi Maklumat (Teknikal) berperanan dan bertanggungjawab kepada perkara berikut : a. Mengurus keseluruhan program-program keselamatan ICT Yayasan Pahang; b. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber Yayasan Pahang kepada semua pengguna; c. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber Yayasan Pahang; d. Menjalankan pengurusan risiko; e. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta	PPTM (Teknikal)

menyediakan langkah-langkah perlindungan yang bersesuaian; g. Melaporkan insiden keselamatan ICT kepada ICTSO; h. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; i. Membantu dalam menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan j. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020105 PENTADBIR SISTEM APLIKASI	**TANGGUNGJAWAB**
Penolong Pegawai Teknologi Maklumat (Aplikasi) di Unit Teknologi Maklumat adalah merupakan Pentadbir Sistem Aplikasi Yayasan Pahang. Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber Yayasan Pahang; c. Memantau aktiviti capaian harian sistem aplikasi pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menganalisis dan menyimpan rekod jejak audit; f. Menyediakan laporan mengenai aktiviti capaian secara berkala; g. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; h. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; i. Memastikan hotfix dan patch yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman virus dan penggodam; j. Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pengujudan akaun pengguna ke atas setiap sistem aplikasi;	PPTM (Aplikasi)

k. Memastikan backup sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual; l. Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; m. Melaporkan kepada CERT Pahang jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;	
020106 PENTADBIR TEKNIKAL DAN KOMUNIKASI	**TANGGUNGJAWAB**
Penolong Pegawai Teknologi Maklumat (Teknikal) di Unit Teknologi Maklumat adalah merupakan Pentadbir Teknikal dan Komunikasi ICT Yayasan Pahang. Peranan dan tanggungjawab Pentadbir adalah seperti berikut : a. Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian Wireless Yayasan Pahang (YPNet) 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 dan sebarang kerosakan perkakasan sokongan rangkaian 1PahangNet; e. Memantau penggunaan rangkaian dan melaporkan kepada CERT Pahang sekiranya berlaku penyalahgunaan sumber rangkaian; f. Mewartakan polisi dan garis panduan penggunaan rangkaian 1PahangNet kepada pengguna rangkaian; g. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian 1PahangNet secara tidak sah; h. Memastikan perisian antivirus dipasang pada Aset ICT yang menggunakan rangkaian 1PahangNet; dan i. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	PPTM (teknikal)
020107 PENTADBIR LAMAN WEB (WEBMASTER)	**TANGGUNGJAWAB**
Juruteknik di Unit Teknologi Maklumat adalah merupakan Pentadbir Laman Web Rasmi Kerajaan Negeri Pahang. Peranan dan tanggungjawab pentadbir Laman Web adalah seperti berikut:	Juruteknik Komputer

a. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan penalaan 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/unit ke web server; e. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; f. Melaporkan sebarang pelanggaran keselamatan laman portal kepada CERT Pahang.	
020108 PENTADBIR E-MEL	**TANGGUNGJAWAB**
Juruteknik Komputer di Unit Teknologi Maklumat adalah merupakan Pentadbir E-Mel Yayasan Pahang. Peranan dan tanggungjawab pentadbir E-Mel adalah seperti berikut: a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar Polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan; d. Melaksanakan jadual penstoran dan pengarkiban e-mel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; e. Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; f. Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam;	Juruteknik Komputer

g. Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala patches terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; h. Memantau status storan e-mel Pengurusan Atasan Yayasan Pahang dan memastikan e-mel Pengurusan Atasan Yayasan Pahang sentiasa tersedia untuk transaksi e-mel; i. Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7; j. Memastikan agar keupayaan mail relay hanya boleh digunakan untuk server atau aplikasi dalaman Yayasan Pahang sahaja bagi tujuan keselamatan; k. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel Pahang; dan l. Memastikan pengguna e-mel Pahang berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel Pahang dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	
020109 PEGAWAI ASET ICT	**TANGGUNGJAWAB**
Penolong Pegawai Teknologi Maklumat di Unit Teknologi Maklumat adalah merupakan Pegawai Aset ICT yang membantu Pegawai Aset Yayasan Pahang bagi pengurusan Aset ICT. Perlantikan ini dibuat oleh Pengurus Besar Yayasan Pahang. Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut : a. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; b. Memastikan Aset ICT milik Yayasan Pahang dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c. Memastikan Aset milik Yayasan Pahang dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut; d. Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin; e. Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan	PPTM (teknikal)

f. Memastikan Aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	
020110 PENGURUS PUSAT DATA DAN DISASTER RECOVERY CENTER (DRC)	**TANGGUNGJAWAB**
Penolong Pegawai Teknologi Maklumat di Unit Teknologi Maklumat adalah merupakan Pegawai yang menguruskan operasi Pusat Data dan Disaster Recovery Center (DRC) Yayasan Pahang. Peranan dan tanggungjawab pegawai adalah seperti berikut : a. Memastikan Operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7; b. Merancang dan menyelia pelaksanaan simulasi Disaster Recovery Plan (DRP) Yayasan Pahang; c. Pengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data Yayasan Pahang; d. Memastikan Operasi Infrastruktur Virtualisasi di Pusat Data dan DRC berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; e. Memastikan Operasi Backup / Restore Data (Auto Backup Script ke NAS, Symantec Netbackup, ArcServe) berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; f. Memantau Aset ICT sokongan dan Fasiliti Sokongan (Precision Aircon, Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar24 x 7; g. Menguruskan permohonan baru dan pengemaskinian server dan Virtual Machine bagi sistem aplikasi baru di Pusat Data dan DRC; h. Melaksanakan housekeeping keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server; dan pusat data dan i. Menguruskan Khidmat Sokongan Operasi Server dari segi Penerimaan, Penyediaan, Penyelenggaraan, Waranti, Pengeluaran dan Pelupusan.	PPTM (teknikal)
020111 MEJA BANTUAN ICT	**TANGGUNGJAWAB**
Peranan dan tanggungjawab Personel Meja Bantuan ICT adalah : a. Memberi bantuan segera kepada pengguna berkaitan masalah ICT	Personel Meja Bantuan ICT

yang dihadapi ; b. Perkhidmatan bantuan peringkat pertama bagi sebarang masalah ICT ; dan c. Mengagihkan masalah ICT kepada personel bertanggungjawab untuk penyelesaian.	
020112 PENGGUNA	**TANGGUNGJAWAB**
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber Yayasan Pahang; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Lulus tapisan keselamatan; d. Melaksanakan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat Kerajaan Negeri Pahang; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 3. Menentukan maklumat sedia untuk digunakan; 4. Menjaga kerahsiaan kata laluan; 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; 6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 7. Menjaga kerahsiaan bagi setiap langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Unit Teknologi Maklumat dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. Menandatangani surat akuan pematuhan Polisi Keselamatan Siber Yayasan Pahang sebagaimana Lampiran 1	Pengguna

020113 PASUKAN CERT PAHANG	TANGGUNGJAWAB
Keanggotaan CERT Pahang adalah seperti berikut: (a) Pengarah CERT : ICTSO (b) Pengurus CERT : KPS(O) (c) Ahli-ahli lain : i. PSUK (Operasi), BTM ii. PSU (Portal), BTM iii. PPTMK Tertinggi (Pusat Data), BTM iv. PPTMK (Komunikasi), BTM v. PPTMK (Aplikasi), BTM vi. PPTM (Teknikal dan Komunikasi), BTM Keahlian ini perlu mendapat kelulusan dari CIO Pejabat Setiausaha Kerajaan Negeri Pahang. Senarai dan pertukaran ahli akan dikemukakan kepada MAMPU untuk tindakan selanjutnya. Laporan berkaitan keselamatan ICT akan dibentangkan secara tetap dalam Mesyuarat Jawatankuasa Pemandu ICT Negeri. Tanggungjawab CERT Pahang meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialami oleh agensi di bawah kawalannya seperti berikut : (a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; (b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minima; (d) Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya; (e) Menasihatkan agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; (f) Menyebarkan makluman berkaitan dengan agensi di bawah kawalannya; dan (g) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT Pahang

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	**TANGGUNGJAWAB**
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 Polisi Keselamatan Siber Yayasan Pahang; 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 Yayasan Pahang 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. Polisi Keselamatan Siber Yayasan Pahang; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f) Menandatangani Surat Akuan Pematuhan Akta Rahsia Rasmi 1972 dan Polisi Keselamatan Siber Yayasan Pahang sebagaimana Lampiran 5.	Semua

BIDANG 03 KAWALAN DAN PENGELASAN ASET

0301 AKAUNTABILITI ASET

Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Yayasan Pahang.

030101 INVENTORI ASET	TANGGUNGJAWAB
Memastikan semua aset ICT Yayasan Pahang hendaklah diberi perlindungan yang bersesuaian oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan semua aset dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan aset bernilai rendah serta sentiasa dikemaskini ; b. Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja ; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Yayasan Pahang dan di Jabatan lain; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset ICT & Semua

0302 PENGELASAN DAN PENGENDALIAN MAKLUMAT

Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

030201 PENGELASAN MAKLUMAT	TANGGUNGJAWAB
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; atau d. Terhad.	Semua

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

BIDANG 04 KESELAMATAN SUMBER MANUSIA

0401 KESELAMATAN ICT DALAM TUGAS HARIAN

Objektif : Untuk memastikan semua sumber manusia yang terlibat termasuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga Yayasan Pahang hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

040101 SEBELUM BERKHIDMAT	TANGGUNGJAWAB
Perkara-perkara yang mesti dipatuhi termasuk yang berikut : a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan Yayasan Pahang serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan Yayasan Pahang 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; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

040102 DALAM PERKHIDMATAN	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Memastikan pegawai dan kakitangan Yayasan Pahang serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Yayasan Pahang; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT Yayasan Pahang secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;	Semua

c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan Yayasan Pahang serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh Yayasan Pahang; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus ICT umum yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan Yayasan Pahang.	
040103 BERTUKAR ATAU TAMAT PERKHIDMATAN	**TANGGUNGJAWAB**
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT Yayasan Pahang dikembalikan kepada Yayasan Pahang mengikut peraturan dan/atau terma yang ditetapkan; b. Mengemaskini semua dokumentasi berkaitan pegawai yang bertukar atau tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan Yayasan Pahang; dan c. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Yayasan Pahang.	Semua

BIDANG 05 KESELAMATAN FIZIKAL

0501 KESELAMATAN KAWASAN	
Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 KAWALAN KAWASAN	**TANGGUNGJAWAB**
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan 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; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK), CIO, ICTSO, Pegawai Aset ICT dan JK Aset dan Bangunan Yayasan Pahang.

050102 KAWALAN MASUK FIZIKAL	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pengguna Yayasan Pahang hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan kembali kepada jabatan apabila pengguna berhenti, bertukar atau bersara; c. Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di Lobi Utama Yayasan Pahang terlebih dahulu dan hendaklah dikembalikan semula selepas tamat lawatan; d. Kehilangan pas mestilah dilaporkan dengan segera; dan	Semua dan pelawat

050103 KAWASAN LARANGAN	TANGGUNGJAWAB
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di Yayasan Pahang adalah : ; a) Bilik Operasi Kewangan Yayasan Pahang; b) Bilik Pengurus Besar Yayasan Pahang; c) Stor Peralatan ICT; d) Pusat Data dan Disaster Recovery Center (DRC); e) Bilik Kawalan CCTV; dan f) Bilik Rak Rangkaian YPNet. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua dan PIC bilik-bilik berkenaan

0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050201 PERALATAN ICT	**TANGGUNGJAWAB**
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 Pegawai Aset ICT / Ketua Jabatan; e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; 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) 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 disokong oleh 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, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan tanpa henti mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari premis Agensi, perlulah mendapat kelulusan Pegawai Aset ICT / Ketua Jabatan dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai	Semua

Aset ICT / Ketua Jabatan 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 Pegawai Aset ICT / Ketua Jabatan; p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Aduan Yayasan Pahang: (http://www.yp.org.my/eaduan) untuk dibaik pulih; q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan pada semua Aset ICT. 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 Pegawai Aset 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 Unit Teknologi Maklumat Yayasan Pahang; dan w) 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	**TANGGUNGJAWAB**
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 storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.	Semua

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) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e) Akses dan pergerakan media storan hendaklah direkodkan; f) Perkakasan data backup hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan atau penduaan (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Sebarang maklumat sulit dan rahsia yang disimpan di dalam media storan perlulah dibuat enkripsi; i) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 MEDIA TANDATANGAN DIGITAL	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada Unit Teknologi Maklumat Yayasan Pahang untuk tindakan seterusnya.	Semua
050204 MEDIA PERISIAN DAN APLIKASI	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan	Semua

pada Peralatan ICT; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO / ICTSO; 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.	
050205 PENYELENGGARAAN PERKAKASAN	**TANGGUNGJAWAB**
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggarakan 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; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset ICT / Ketua Jabatan.	Pegawai Aset ICT dan Unit Teknologi Maklumat Yayasan Pahang
050206 PEMINJAMAN ASET ICT BAGI KEGUNAAN DI LUAR PEJABAT	**TANGGUNGJAWAB**
Aset ICT yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Aset ICT merangkumi peralatan, perisian dan maklumat ICT. Langkah-langkah berikut boleh diambil untuk menjamin	Semua

keselamatan Aset ICT : a. Aset ICT yang dibawa keluar pejabat mestilah mendapat kelulusan Pegawai Aset ICT atau Pengurus Bahagian/Unit atau Ketua Jabatan dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan; c. Peminjam perlu bertanggungjawab terhadap keselamatan Aset ICT yang dipinjam; d. Aset ICT perlu dilindungi dan dikawal sepanjang masa; e. Penyimpanan atau penempatan Aset ICT perlu mengambil kira ciri-ciri keselamatan lokasi yang bersesuaian; dan f. Sebarang kehilangan semasa peminjaman Aset ICT tersebut perlulah dilaporkan kepada pihak Berkuasa dan kepada Pegawai Aset ICT / Ketua Jabatan.	
050207 PENGENDALIAN PERALATAN LUAR YANG DIBAWA MASUK	**TANGGUNGJAWAB**
Bagi peralatan yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT Yayasan Pahang; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh Yayasan Pahang bagi membawa masuk / keluar sebarang peralatan; dan c. Memeriksa dan memastikan peralatan ICT dari luar yang dibawa masuk dan ingin dibawa keluar setelah selesai tugasan tidak mengandungi maklumat kerajaan. Jika ada, ia perlu disalin dan dihapuskan melainkan mendapat kebenaran daripada Pegawai di tempat tugas dilaksanakan.	Semua
050208 PELUPUSAN PERKAKASAN	**TANGGUNGJAWAB**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Yayasan Pahang dan ditempatkan di bahagian/unit	Pegawai Aset ICT

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan di agensi dan jabatan masing-masing. 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, degauzing atau pembakaran;

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

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

d) Pegawai Aset ICT 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 Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset;

g) Pelupusan peralatan ICT Yayasan Pahang hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

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, motherboard dan sebagainya;

   ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke lokasi berlainan tanpa kebenaran;

   iii. Memindah keluar dari Agensi atau Jabatan bagi mana-mana peralatan ICT milik Yayasan Pahang yang hendak dilupuskan tanpa kebenaran;

   iv. Melupuskan sendiri peralatan ICT Yayasan Pahang kerana kerja-kerja pelupusan di bawah tanggungjawab Yayasan Pahang; dan

   v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumb drive atau external hard

disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

0503 KESELAMATAN PERSEKITARAN

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

050301 KAWALAN PERSEKITARAN	TANGGUNGJAWAB
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Unit Aset dan Bangunan Yayasan Pahang. 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 kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran 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	Semua dan JK Aset dan Bangunan Yayasan Pahang

050302 BEKALAN KUASA	TANGGUNGJAWAB
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	Unit Teknologi Maklumat dan JK Aset dan Bangunan Yayasan Pahang

elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (Uninterruptable Power Supply) 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.	
050303 KABEL	**TANGGUNGJAWAB**
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 wire tapping; dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Unit Teknologi Maklumat
050304 PROSEDUR KECEMASAN	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan; b. Mewujud, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; c. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Yayasan Pahang yang dilantik.	Semua

0504 KESELAMATAN DOKUMEN	
Objektif: Melindungi maklumat Yayasan Pahang dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 DOKUMEN	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut 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; dan e. Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI

0601 PENGURUSAN PROSEDUR OPERASI	
Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan	
060101 PENGENDALIAN PROSEDUR	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta 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	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini 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; dan 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	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 dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah dilaksanakan dalam persekitaran development server sebelum dimasukkan ke dalam production server yang menggunapakai persekitaran yang sama.	ICTSO
0602 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 PERKHIDMATAN PENYAMPAIAN	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu 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.	Semua

0603 PERANCANGAN DAN PENERIMAAN SISTEM	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 PERANCANGAN KAPASITI	**TANGGUNGJAWAB**
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.	ICTSO, Pegawai Aset ICT
060302 PENERIMAAN SISTEM	**TANGGUNGJAWAB**
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem Aplikasi
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	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, 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. Memastikan perisian antivirus mempunyai pengurusan berpusat bagi memudahkan penetapan polisi dan penyediaan laporan jika berlaku virus outbreak dalam rangkaian; d. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya serta dilaksanakan secara berkala; e. Mengemas kini antivirus dengan pattern terkini;	Pentadbir Teknikal dan Komunikasi

f. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; 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.	
060402 PERLINDUNGAN DARI MOBILE CODE	**TANGGUNGJAWAB**
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	**TANGGUNGJAWAB**
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	Pentadbir Sistem Aplikasi

dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. d. Menyimpan sekurang-kurangnya tiga generasi backup; dan e. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	
0606 PENGURUSAN RANGKAIAN Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 KAWALAN INFRASTRUKTUR RANGKAIAN	**TANGGUNGJAWAB**
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Tanggungjawab atau kerja-kerja operasi rangkaian 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; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses Factory Acceptance Check (FAC) semasa pemasangan dan konfigurasi; e. Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk dalam 1PahangNet hendaklah melalui firewall di bawah kawalan Yayasan Pahang; g. Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran Ketua Jabatan; h. Memasang perisian Intrusion Prevention System (IPS) atau Web Application Firewall (WAF) mengikut kesesuaian bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat di dalam 1PahangNet; i. Memasang Web Content Filtering untuk menyekat aktiviti Web Surfing yang dilarang semasa waktu kerja;	ICTSO, Pentadbir Teknikal dan Komunikasi

j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Yayasan Pahang adalah tidak dibenarkan; a. Semua pengguna hanya dibenarkan menggunakan rangkaian YP b. Net sahaja dan penggunaan rangkaian lain seperti 3G, 4G, HTE, LTE, ADSL dan Wimax adalah dilarang sama sekali kecuali telah mendapatkan kebenaran atas sebab tertentu dan penggunaannya perlulah di bawah seliaan serta pemantauan ketua bahagian/unit masing-masing; c. Sebarang penggunaan rangkaian komunikasi daripada agensi lain (contoh : EGNet, NRENet) perlulah mendapat khidmat nasihat daripada Pentadbir Teknikal dan Komunikasi terlebih dahulu dan pelaksanaan secara berpusat perlulah menjadi keutamaan; dan d. 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	**TANGGUNGJAWAB**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik Aset ICT terlebih dahulu.	Semua
060702 PROSEDUR PENGENDALIAN MEDIA	**TANGGUNGJAWAB**
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut : 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	Semua

mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
060703 KESELAMATAN SISTEM DOKUMENTASI	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut : a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
0608 PENGURUSAN PERTUKARAN MAKLUMAT Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara Yayasan Pahang dan agensi luar terjamin	
060801 PERTUKARAN MAKLUMAT	**TANGGUNGJAWAB**
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 Yayasan Pahang dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari Yayasan Pahang; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060802 PENGURUSAN MEL ELEKTRONIK (E-MEL)	**TANGGUNGJAWAB**
Penggunaan e-mel di Yayasan Pahang hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika	Semua

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 berkuat kuasa.

Peraturan Penggunaan Emel Rasmi Kerajaan Negeri Pahang juga menjadi rujukan kepada kaedah pengurusan Mel Elektronik ini.

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut :

a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Yayasan Pahang sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Yayasan Pahang;
c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) atau mengikut polisi yang ditetapkan agensi semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;
h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;
j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;
k. Mengambil tindakan dan memberi maklum balas terhadap e-mel

dengan cepat dan mengambil tindakan segera; l. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti Yahoo Mail, Gmail, Hotmail dan sebagainya) tidak digunakan untuk tujuan rasmi; dan m. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
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	**TANGGUNGJAWAB**
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. 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.	Semua
060902 MAKLUMAT UMUM	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan	Semua

c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web	
0610 PEMANTAUAN Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan	
061001 PENGAUDITAN DAN FORENSIK ICT	**TANGGUNGJAWAB**
Perkara-perkara berikut perlulah direkod dan dianalisis oleh Pasukan CERT Pahang : a. Sebarang percubaan pencerobohan kepada sistem ICT; b. Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery), penipuan (phising), pencerobohan (intrusion), ancaman (threats) dan kehilangan fizikal (physical loss); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem Aplikasi. Langkah-langkah yang perlu diambil adalah seperti berikut : a. Unit Teknologi Maklumat akan menentukan prosedur pengumpulan bahan bukti (hard disk/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan	CIO, Pengurusan Tertinggi Yayasan Pahang, ICTSO

yang akan disediakan; b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan dan berstatus SULIT.	
061002 JEJAK AUDIT	**TANGGUNGJAWAB**
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; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Semua Pentadbir ICT 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.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi
061003 SISTEM LOG	**TANGGUNGJAWAB**
Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti	Pentadbir Sistem

berikut : i. fail log sistem pengoperasian; ii. fail log servis (web, e-mel); iii. fail log aplikasi (audit trail); dan iv. fail log rangkaian (switch, firewall, IPS) Pentadbir Sistem Aplikasi, Pentadbir Laman Web dan Pentadbir E-Mel 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; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada Unit Teknologi Maklumat untuk dibawa ke Penguruan Tertinggi Yayasan Pahang.	Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi
061004 PEMANTAUAN LOG	**TANGGUNGJAWAB**
Pentadbir ICT hendaklah melaksanakan perkara-perkara 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. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat atau domain keselamatan perlu diselaraskan dengan satu sumber	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi

waktu yang dipersetujui.	

BIDANG 07 KAWALAN CAPAIAN

0701 POLISI KAWALAN CAPAIAN	
Objektif : Memahami capaian ke atas maklumat	
070101 KEPERLUAN KAWALAN CAPAIAN	**TANGGUNGJAWAB**
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong Polisi 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.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi

0702 PENGURUSAN CAPAIAN PENGGUNA	
Objektif : Mengawal capaian pengguna ke atas aset ICT Yayasan Pahang.	
070201 AKAUN PENGGUNA	**TANGGUNGJAWAB**
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi : a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi

e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Sistem Aplikasi boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii) Bertukar bidang tugas kerja; iii) Bersara; atau iv) Ditamatkan perkhidmatan	
070202 HAK CAPAIAN	**TANGGUNGJAWAB**
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel,, Pentadbir Teknikal dan Komunikasi
070203 PENGURUSAN KATA LALUAN	**TANGGUNGJAWAB**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Yayasan Pahang seperti berikut : a. Dalam apa 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 dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; 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 guna sama;	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi

f. Kata laluan 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. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j. Had cubaan kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa selama 30 minit (mengikut kesesuaian sistem) atau setelah diset semula oleh Pentadbir Sistem Aplikasi; k. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; l. Mengelakkan penggunaan semula kata laluan yang telah digunakan; dan m. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
070204 CLEAR DESK DAN CLEAR SCREEN	**TANGGUNGJAWAB**
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk dan Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pentadbir Teknikal dan Komunikasi

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

0703 KAWALAN CAPAIAN RANGKAIAN

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

070301 CAPAIAN RANGKAIAN	TANGGUNGJAWAB
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan : a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian YpNet, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Teknikal dan Komunikasi

070302 CAPAIAN INTERNET	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Penggunaan Internet di dalam YPNet hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Yayasan Pahang; 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	Pentadbir Teknikal dan Komunikasi

(video conferencing, video streaming, chat, downloading) adalah perlu bagi menguruskan penggunaan jalur lebar (bandwidth) yang maksimum dan lebih berkesan;

d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pentadbir Teknikal dan Komunikasi berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya setelah mendapat maklumat dari Ketua Jabatan;

e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengurus Bahagian/Unit/Jabatan/ pegawai yang diberi kuasa;

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

g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengurus Bahagian/Unit/Jabatan/ pegawai yang diberi kuasa 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 Yayasan Pahang;

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 CIO terlebih dahulu tertakluk kepada Polisi dan peraturan yang telah ditetapkan;

k. Penggunaan modem (milik persendirian) untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali di pejabat kecuali dengan kebenaran seperti di Lampiran 3; dan

l. 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; 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	**TANGGUNGJAWAB**
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; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut : a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan c. Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk	Pegawai Aset ICT, Pentadbir Teknikal dan Komunikasi

setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Mengehadkan dan mengawal penggunaan program; dan d. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070402 KAD PINTAR	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Pegawai yang bertanggungjawab di Yayasan Pahang.	Semua
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	TANGGUNGJAWAB
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi : a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem dan aplikasi 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; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

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	**TANGGUNGJAWAB**
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	**TANGGUNGJAWAB**

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 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	TANGGUNGJAWAB
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 serta 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.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

080102 PENGESAHAN DATA INPUT DAN OUTPUT	TANGGUNGJAWAB
Perkara yang perlu dipatuhi adalah seperti berikut : a. Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

0802 KAWALAN KRIPTOGRAFI	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 ENKRIPSI	**TANGGUNGJAWAB**
Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa	Semua
080202 TANDATANGAN DIGITAL	**TANGGUNGJAWAB**
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik dengan kebenaran bertulis dari pemilik proses.	Semua
080203 PENGURUSAN INFRASTRUKTUR KUNCI AWAM (PKI)	**TANGGUNGJAWAB**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
0803 FAIL SISTEM	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 KAWALAN FAIL SISTEM	**TANGGUNGJAWAB**
Perkara yang perlu dipatuhi adalah seperti berikut : a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pembangun sistem aplikasi atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Pengemaskinian kod atau atur cara yang melibatkan proses kerja sistem 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; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

0804 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 KAWALAN PERUBAHAN	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja. b. Keperluan dan kesesuaian perubahan terhadap sistem pengoperasian dan perisian sokongan perlu dikaji terlebih dahulu. c. Sebarang perubahan sistem pengoperasian dan perisian sokongan perlu diuji dahulu di dalam development server sebelum dipasang di dalam server sebenar. d. Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi
080402 PEMBANGUNAN PERISIAN SECARA OUTSOURCE	**TANGGUNGJAWAB**
Pembangunan aplikasi secara outsource perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan Negeri Pahang.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

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	**TANGGUNGJAWAB**
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mendapatkan maklumat teknikal keterdedahan (vulnerabilities) yang tepat 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.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, Pentadbir Teknikal dan Komunikasi

BIDANG 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	**TANGGUNGJAWAB**
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 Polisi Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada CERT Pahang 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 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 Yayasan Pahang sepertimana Lampiran 2. Prosedur pelaporan insiden keselamatan ICT berdasarkan : a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan c. Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT Computer Emergency Response Team (CERT) Pahang.	Semua

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	**TANGGUNGJAWAB**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Yayasan Pahang. 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 kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO, PPTM(Teknikal), CERT Pahang

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 POLISI KESINAMBUNGAN PERKHIDMATAN	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)	**TANGGUNGJAWAB**
Pengurusan Kesinambungan Perkhidmatan adalah proses pengurusan holistik yang mengenalpasti ancaman dan risiko, impak ancaman dan risiko tersebut terhadap fungsi kritikal jabatan dan penentuan strategi bagi memastikan perkhidmatan jabatan tetap dapat diteruskan walaupun berlaku gangguan/bencana. Pelan Pengurusan Kesinambungan Perkhidmatan (BCP) adalah pelan menyeluruh bagi menyedia dan memulihkan jabatan agar dapat meneruskan perkhidmatan dalam tempoh masa sesingkat mungkin semasa bencana atau gangguan. Pelan Kesinambungan Perkhidmatan (BCP) terdiri daripada 4 sub-pelan berikut: a. Pelan Tindakbalas Kecemasan (ERP) b. Pelan Pemulihan Bencana (DRP) c. Pelan Komunikasi Krisis (CCP) d. Pelan Simulasi Pelan ini mestilah diluluskan oleh Pengurusan Tertinggi dan perkara-perkara berikut perlu diberi perhatian : a. Mengenal pasti 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;	Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT), Critical Communication Team (CCT) Yayasan Pahang

e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

f. Membuat backup dan pengujian ke atas data *backup (restore*); dan

g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

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

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

b. Senarai personel Yayasan Pahang 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;

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

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan mengikut kesesuaian.

Salinan pelan BCP 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 BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

Yayasan Pahang hendaklah memastikan salinan pelan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

BIDANG 11 PEMATUHAN

1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Polisi Keselamatan Siber Yayasan Pahang.	
110101 PEMATUHAN POLISI	**TANGGUNGJAWAB**
Setiap pengguna di Yayasan Pahang hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber Yayasan Pahang dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di Yayasan Pahang termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua /Bahagian/Unit/Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT Yayasan Pahang selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Yayasan Pahang.	Semua
110102 PEMATUHAN DENGAN POLISI , PIAWAIAN DAN KEPERLUAN TEKNIKAL	**TANGGUNGJAWAB**
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi Polisi , piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

110103 PEMATUHAN KEPERLUAN AUDIT	TANGGUNGJAWAB
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	**TANGGUNGJAWAB**
Senarai perundangan dan peraturan yang perlu dipatuhi oleh pengguna di Yayasan Pahang adalah seperti di Lampiran 4.	Semua
110105 PERLANGGARAN POLISI	**TANGGUNGJAWAB**
Pelanggaran Polisi Keselamatan Siber Yayasan Pahang boleh dikenakan tindakan tatatertib.	Semua

GLOSARI

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam angka masa yang ditetapkan.
CIO	Chief Information Officer Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
CERT Pahang	Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi bawah pentadbiran Kerajaan Negeri Pahang
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

GLOSARI	
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen Kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	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.

GLOSARI	
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.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
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.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	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.

GLOSARI	
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER YAYASAN PAHANG

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER YAYASAN PAHANG

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Unit / Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Yayasan Pahang; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

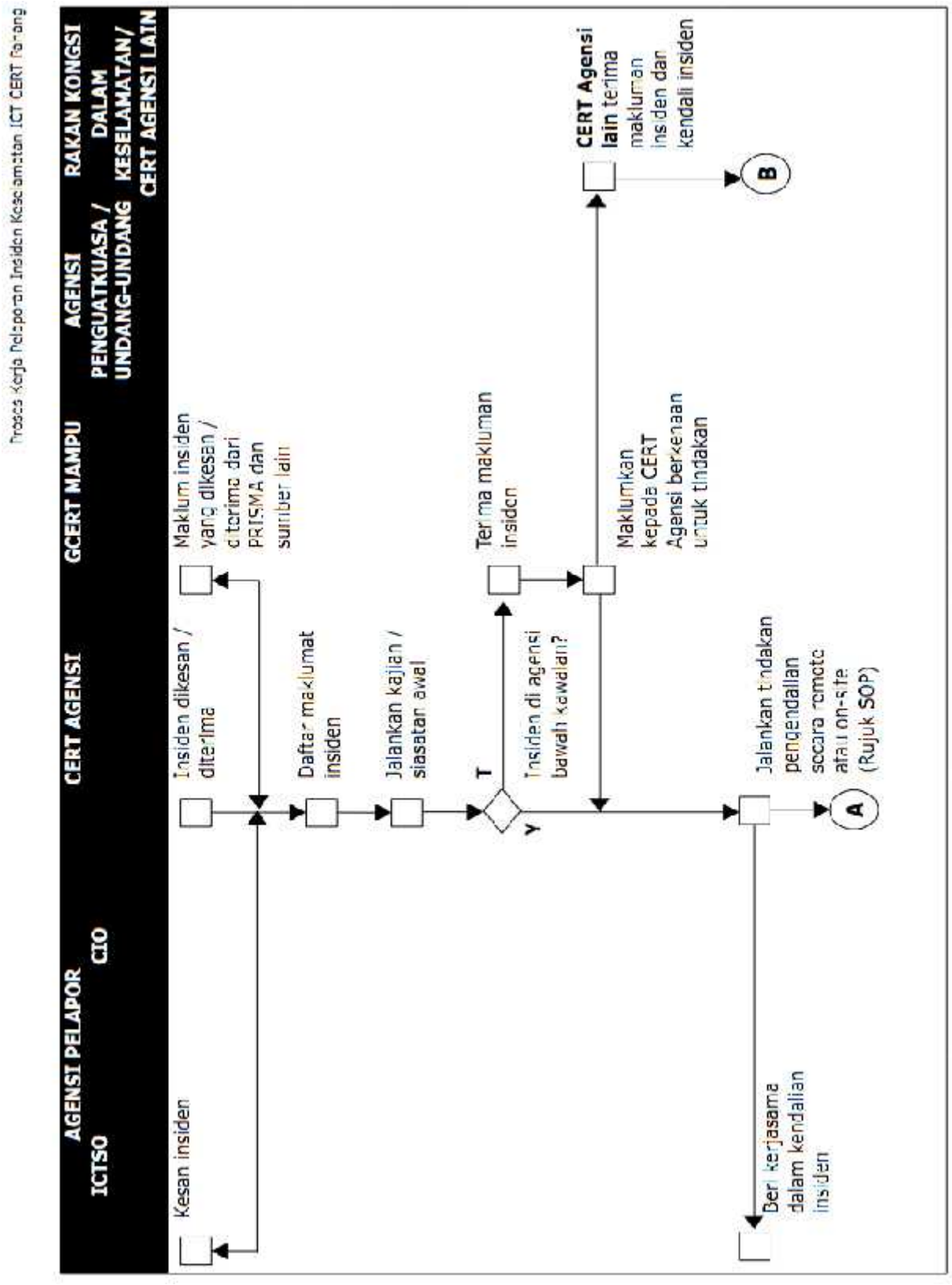
Tanda tangan : .....

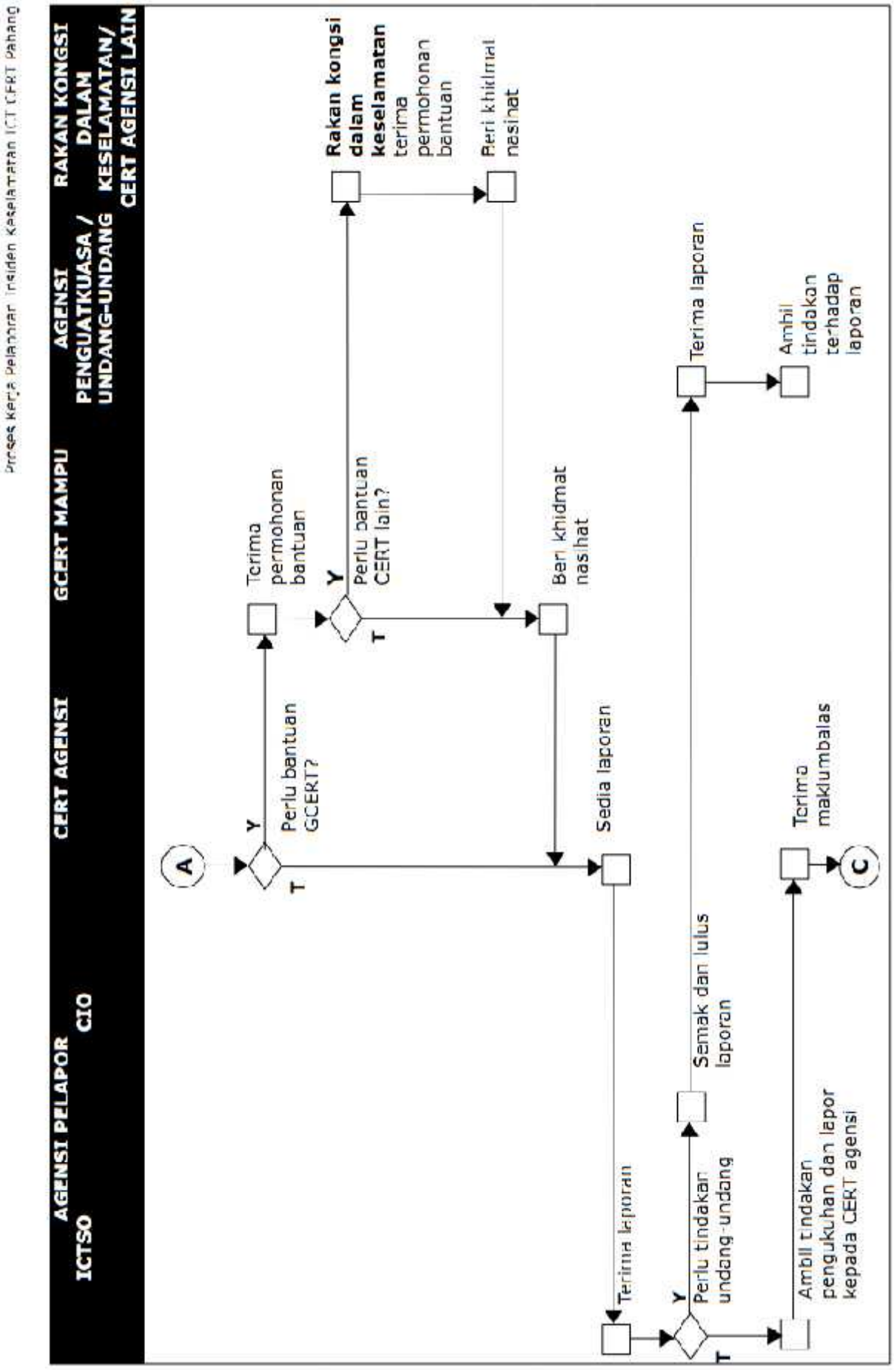
Tarikh : .....

Rujukan:

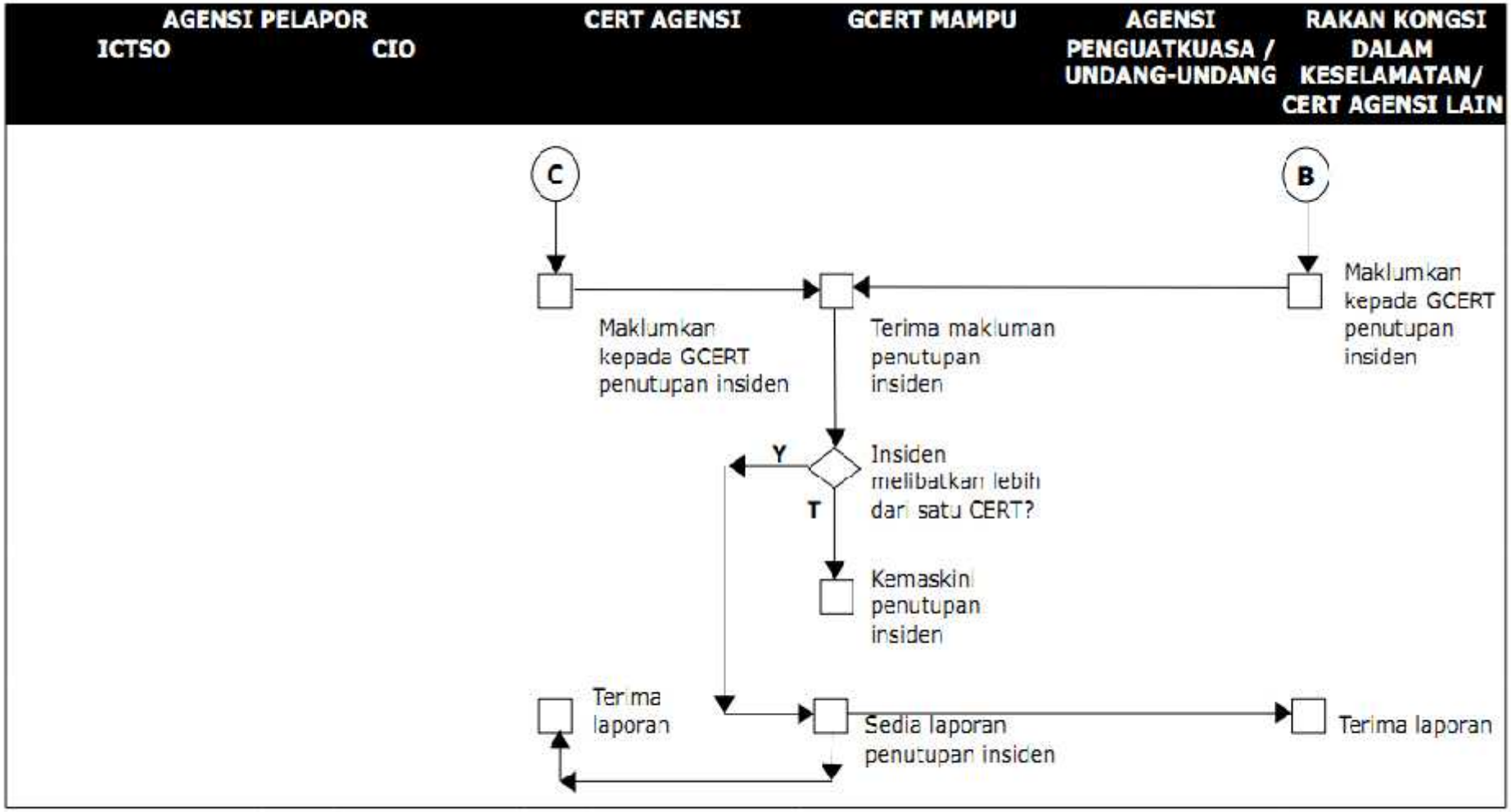
Sila layari POLISI KESELAMATAN SIBER YAYASAN PAHANG di http://www.yp.org.my/

LAMPIRAN 2 : PELAPORAN INSIDEN KESELAMATAN ICT CERT PAHANG




Proses Kerja Pelaporan Insiden Keselamatan ICT CERT Pahang
AGENSI PELAPOR
ICTSO
CIO
CERT AGENSI
GCERT MAMPU
AGENSI PENGUATKUASA / UNDANG-UNDANG
RAKAN KONGSI DALAM KESELAMATAN/ CERT AGENSI LAIN
A
Perlu bantuan GCERT?
Y
T
Terima permohonan bantuan
Perlu bantuan CERT lain?
Y
T
Rakan kongsi dalam keselamatan terima permohonan bantuan
Beri khidmat nasihat
Beri khidmat nasihat
Sedia laporan
Terima laporan
Perlu tindakan undang-undang
Y
T
Semak dan lulus laporan
Ambil tindakan pengukuhan dan lapor kepada CERT agensi
Terima laporan
Ambil tindakan terhadap laporan
Terima maklumbalas
C

Proses Kerja Pelaporan Insiden Keselamatan ICT CERT Pahang



KETERANGAN :
CERT AGENSI – Computer Emergency Response Team Negeri Pahang
CIO – Chief Information Officer yang dilantik disetiap agensi
ICTSO – Information Communication Technology Security Officer (Pegawai Keselamatan ICT yang dilantik di setiap agensi)

LAMPIRAN 3 : PERMOHONAN KEBENARAN UNTUK MENGGUNAKAN MODEM

PERMOHONAN KEBENARAN UNTUK MENGGUNAKAN MODEM PERIBADI
BAGI TUJUAN SAMBUNGAN KE INTERNET

Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Organisasi : .....

Saya dengan ini memohon kebenaran daripada Pengurus Teknologi Maklumat untuk menggunakan modem peribadi bagi tujuan seperti berikut:

_____

_____

Saya juga sedar bahawa saya terikat dengan peraturan-peraturan seperti yang telah ditetapkan di dalam dokumen Polisi Keselamatan Siber (PKS) Yayasan Pahang. Dan jika saya ingkar kepada peruntukan-peruntukan tersebut, maka tindakan sewajarnya boleh diambil ke atas diri saya. Kebenaran ini juga tertakluk kepada tiga (3) syarat berikut :

i. Memastikan perisian antivirus sentiasa aktif (activated) dan dikemaskini disamping turut melakukan imbasan ke atas media storan yang digunakan
ii. Memasang dan menggunakan hanya perisian yang tulen
iii. Tidak menyambungkan Notebook/Netbook/Mobile Devices kepada rangkaian dalaman Jabatan (wired/wireless) dan modem peribadi secara serentak

Tandatangan : .....
Tarikh : .....

Pengesahan Pengurus Teknologi Maklumat

.....
(Nama Pengurus Teknologi Maklumat)
b.p. Yayasan Pahang

Tarikh: .....

LAMPIRAN 4 : SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Polisi Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
4. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
8. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
9. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
10. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
11. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
12. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
13. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
14. Pekeliling 1PP AM 2 : Tatacara Pengurusan Aset Alih Kerajaan (2.1 – 2.7)
15. Akta Tandatangan Digital 1997;
16. Akta Rahsia Rasmi 1972;
17. Akta Jenayah Komputer 1997;
18. Akta Hak Cipta (Pindaan) Tahun 1997;
19. Akta Komunikasi dan Multimedia 1998;
20. Perintah-Perintah Am;

21. Arahan Perbendaharaan;
22. Arahan Teknologi Maklumat 2007;
23. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
24. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.
25. Surat Pekeliling YB SUK Pahang : Bil 01 Tahun 2008 : Perlaksanaan Penggunaan Perisian Open Office.Org di Semua Agensi Dan Pentadbiran Negeri
26. Surat Pekeliling YB SUK Pahang : Bil 02 Tahun 2008 : Perlaksanaan Penggunaan Perisian CADIAN
27. Surat Pekeliling YB SUK Pahang : Bil 05 Tahun 2008 : Arahan Keselamatan Penggunaan Komputer Riba Di Jabatan-jabatan Kerajaan Negeri Pahang
28. Surat Pekeliling YB SUK Pahang : Bil 08 Tahun 2009 : Dasar Keselamatan ICT Pejabat SUK Negeri Pahang
29. Surat Arahan YB SUK Pahang (13 Jan 2011) : Larangan Penggunaan Perisian tidak berlesen di Komputer Milik Kerajaan
30. Surat Arahan YB SUK Pahang (13 Jun 2011) : Pendaftaran Aset Milik Persendirian dan Sumbangan
31. Surat Arahan CIO (21 Apr 2011) : Perkongsian Pencetak di Pejabat SUK Negeri Pahang dan Jabatan Negeri Pahang
32. Surat Arahan (28 Mac 2016) : Pelaksanaan Penyelenggaraan Berjadual Bagi Aset ICT Dan Peraturan Kepada Pemilik Aset ICT Pejabat Setiausaha Kerajaan Pahang
33. Rangka Kerja Keselematan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)

LAMPIRAN 5 : SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER YAYASAN PAHANG

\

PERAKUAN UNTUK DITANDATANGANI BERKENAAN
DENGAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER
YAYASAN PAHANG

NAMA PROJEK :

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi sesuatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi adalah milik Yayasan Pahang dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan atau dengan bertulisan atau secara media elektronik, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis pihak berkuasa yang berkenaan.

Saya juga turut tertakluk di bawah Polisi Keselamatan Siber Yayasan Pahang terkini berkenaan Perkara : Keperluan Keselamatan Kontrak dengan Pihak Ketiga. Selain itu, saya juga telah membaca dan faham serta akan mematuhi polisi lain di dalam Polisi Keselamatan Siber Yayasan Pahang yang berhubungkait dengan urusan ini.

Saya juga dengan ini mewakili ..... mengakui bahawa semua maklumat yang dinyatakan seperti di Lampiran A adalah terlibat secara langsung bagi sebarang urusan yang memerlukan pematuhan akta dan Polisi Keselamatan Siber Yayasan Pahang seperti semua keterangan perenggan di atas. Oleh itu, sesiapa yang tiada dalam senarai Lampiran A tersebut tidak dibenarkan terlibat secara langsung bagi sebarang urusan melibatkan peruntukan Akta Rahsia Rasmi 1972.

* Sila lengkapkan dengan tulisan HURUF BESAR

Tandatangan	Disaksikan oleh :
Nama :	Nama :
No. Kad Pengenalan :	No. Kad Pengenalan :
Jawatan :	Jawatan :
Jabatan/Syarikat :	Jabatan/Syarikat :
Tarikh :	Tarikh :

Alamat Jabatan/Syarikat :

Cop Jabatan/Syarikat :

LAMPIRAN A

SENARAI KAKITANGAN JABATAN / SYARIKAT YANG TERLIBAT DALAM URUSAN ANTARA JABATAN / SYARIKAT ….....

DENGAN YAYASAN PAHANG.

* Sila lengkapkan dengan tulisan HURUF BESAR

BIL	NAMA & JABATAN / JAWATAN SYARIKAT	NO KAD PENGENALAN

Ketua Pegawai Eksekuti (CEO)	Pengurus Besar Yayasan Pahang
Ketua Pegawai Maklumat (CIO)	Pengurus Teknologi Maklumat
Pegawai Keselamatan ICT (ICTSO)	Penolong Pengurus Teknologi Maklumat
Pengurus Pusat Data dan DRC	Penolong Pengurus Teknologi Maklumat
Pegawai Operasi	Penolong Pengurus Pentadbiran
Pentadbir Sistem Aplikasi	Penolong Pegawai Teknologi Maklumat (Aplikasi)
Pentadbir Teknikal dan Komunikasi	Penolong Pegawai Teknologi Maklumat (Teknikal)
Pegawai Aset ICT	Penolong Pegawai Teknologi Maklumat (Teknikal)
Pentadbir Laman Web	Juruteknik Komputer
Pentadbir Emel	Juruteknik Komputer