PENGURUSAN AIR PAHANG BERHAD (200801004468)

POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

MANUAL POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

	RUJ. MANUAL	PKSPAIP/PAIP/01
	TARIKH ISU	01/02/2026
	ISU NO.	01
	SEMAKAN NO.	-

VERSI DOKUMEN

No.Rujukan	:	POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD
Versi	:	Versi 1.0
Tarikh	:	1 FEBRUARI 2026
Disediakan Oleh	:	UNIT TEKNOLOGI MAKLUMAT, JABATAN PERKHIDMATAN STRATEGIK

DISEMAK OLEH :

Tanda tangan :

Nama : Ts. MUHAMMAD HILMI BIN ABDUL HAMID

Jawatan : Pengurus Kanan
Jabatan Perkhidmatan Strategik
Pengurusan Air Pahang Berhad

Tarikh : 10/3/2026

DILULUSKAN OLEH :

Tanda tangan :

Nama : DATO' SAIFUL ZAINI BIN MOHD BOKHARI, D.I.M.P.

Jawatan : KETUA PEGAWAI EKSEKUTIF
PENGURUSAN AIR PAHANG BERHAD

Tarikh : 11/3/2026

MANUAL POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

PENGENALAN

Polisi Keselamatan Siber Pengurusan Air Pahang Berhad (PKS PAIP Berhad) 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 Pengurusan Air Pahang Berhad (PAIP Berhad).

OBJEKTIF

PKS PAIP Berhad diwujudkan untuk menjamin kesinambungan urusan di dalam PAIP Berhad dengan meminimumkan kesan insiden keselamatan ICT.

Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi pentadbiran PAIP Berhad. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Manakala, objektif utama PKS PAIP Berhad ialah seperti berikut:

a. Memastikan kelancaran operasi PAIP Berhad 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 PAIP Berhad.

PENYATAAN 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 PAIP Berhad 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.

PKS PAIP Berhad 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 daripada 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 :

a. Maklumat (contoh: fail, dokumen, data elektronik);

b. Perisian (contoh: aplikasi dan sistem perisian); dan

c. Fizikal (contoh: komputer, peralatan komunikasi dan media penyimpanan
data).

Polisi ini adalah terpakai oleh semua pengguna di PAIP Berhad termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT PAIP Berhad. Aset ICT PAIP Berhad terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS PAIP Berhad 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, PKS PAIP Berhad 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 PAIP Berhad. 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 PAIP Berhad;

(c) Perkhidmatan

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

a. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
b. Sistem halangan akses seperti sistem kad akses; dan
c. Perkhidmatan sokongan seperti kemudahan elektrik, penyaman udara, 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 PAIP Berhad. Contohnya, sistem dokumentasi, prosedur operasi, rekod- rekod PAIP Berhad, 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 PAIP Berhad bagi mencapai visi, 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 PKS PAIP Berhad 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 Akta 854 (Akta Keselamatan Siber 2024);

(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 dipertanggungjawab ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawab ke 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 daripada 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 merangkumitindakan 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, komputer riba, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) Pematuhan

PKS PAIP Berhad 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

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

PAIP Berhad 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 PAIP Berhad 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, kemudahan utiliti, dan sistem - sistem sokongan lain.

PAIP Berhad 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

SINGKATAN DAN TAKRIFAN

Singkatan & Takrifan	
PKS	Polisi Keselamatan Siber
PAIP Berhad	Pengurusan Air Pahang Berhad
CIO	Chief Information Officer (Ketua Jabatan Perkhidmatan Strategik) Pegawai yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer (Ketua Unit Teknologi Maklumat) Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
SSIT	Penolong Pengurus Sokongan Sistem, Infra & Teknologi
PPAS	Penolong Pengurus Pembangunan Aplikasi & Sistem
PSP	Penolong Pengurus Perkhidmatan & Sokongan Pengguna
KJ	Ketua Jabatan
ISMR	Information System Management Representative
PAICT	Pegawai Aset ICT
DRC	Disaster Recovery Center
PAIP CERT	Cyber Security and Emergency Response Teams atau Pasukan Tindak Balas Insiden Keselamatan ICT PAIP. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi bawah pentadbiran Pengurusan Air Pahang Berhad.
JPICT	Pengerusi Jawatankuasa Pemandu ICT PAIP Berhad
PKP	Pelan Kesinambungan Perkhidmatan
GM HR	Pengurus Besar Divisyen Pengurusan dan Sumber Manusia

POLISI KESELAMATAN SIBER PAIP	
01 PEMBANGUNAN DAN PENYELENGGARAAN POLISI	
0101 POLISI KESELAMATAN SIBER	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PAIP Berhad dan perundangan yang berkaitan.	
010101 PELAKSANAAN POLISI	**TANGGUNGJAWAB**
Pelaksanaan Polisi ini akan dijalankan oleh Ketua Pegawai Eksekutif selaku Pengerusi Jawatankuasa Pemandu ICT PAIP Berhad (JPICT) dan dibantu oleh : i. Ketua Jabatan Perkhidmatan Strategik – (CIO) ii. Ketua Unit Teknologi Maklumat – (ICTSO) iii. Ketua Unit Perancangan Strategik iv. Penolong Pengurus Sokongan Sistem, Infra & Teknologi - (SSIT) v. Penolong Pengurus Pembangunan Aplikasi & Sistem – (PPAS) vi. Penolong Pengurus Perkhidmatan & Sokongan Pengguna – (PSP)	Pihak Pengurusan PAIP Berhad

POLISI KESELAMATAN SIBER PAIP	
01 PEMBANGUNAN DAN PENYELENGGARAAN POLISI	
0101 POLISI KESELAMATAN SIBER	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PAIP Berhad dan perundangan yang berkaitan.	
010102 PENYEBARAN POLISI	**TANGGUNGJAWAB**
Polisi ini perlu disebarkan kepada semua pengguna di PAIP Berhad yang menggunapakai (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	Pihak Pengurusan PAIP Berhad

POLISI KESELAMATAN SIBER PAIP	
01 PEMBANGUNAN DAN PENYELENGGARAAN POLISI	
0101 POLISI KESELAMATAN SIBER	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PAIP Berhad dan perundangan yang berkaitan.	
010103 PENYELENGGARAAN POLISI	**TANGGUNGJAWAB**
PKS 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 PKS PAIP Berhad: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT PAIP Berhad (JPICT); c. Maklum kepada semua pengguna perubahan yang telah dipersetujui	ICTSO

POLISI KESELAMATAN SIBER PAIP	
01 PEMBANGUNAN DAN PENYELENGGARAAN POLISI	
0101 POLISI KESELAMATAN SIBER	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PAIP Berhad dan perundangan yang berkaitan.	
010104 PENGECUALIAN POLISI	**TANGGUNGJAWAB**
PKS PAIP Berhad adalah terpakai kepada semua pengguna ICT di PAIP Berhad tanpa pengecualian.	Semua

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020101 PAIP BERHAD	**TANGGUNGJAWAB**
Peranan dan tanggungjawab PAIP Berhad adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan dibawah PKS PAIP Berhad; b. Memastikan semua pengguna mematuhi PKS PAIP Berhad; 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 PKS PAIP Berhad.	PAIP Berhad

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020102 KETUA JABATAN PERKHIDMATAN STRATEGIK (CIO)	**TANGGUNGJAWAB**
Ketua Jabatan Perkhidmatan Strategik adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. 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 PKS PAIP Berhad serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT PAIP Berhad.	CIO

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020103 PENOLONG PENGURUS SOKONGAN SISTEM, INFRA & TEKNOLOGI (SSIT)	**TANGGUNGJAWAB**
Penolong Ketua Unit adalah merupakan SSIT PAIP Berhad. Peranan dan tanggungjawab SSIT adalah seperti berikut : a. Memahami dan mematuhi PKS PAIP Berhad; b. Menguatkuasakan PKS PAIP Berhad; c. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PAIP Berhad; d. Menentukan kawalan akses semua pengguna terhadap aset ICT PAIP Berhad; 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 insiden keselamatan ICT kepada Information System Management Representative (ISMR); g. Menyimpan rekod, bahan bukti, dan laporan terkini mengenai ancaman keselamatan ICT PAIP berhad; h. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar PKS PAIP Berhad	SSIT

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020105 PENOLONG PENGURUS PEMBANGUNAN APLIKASI & SISTEM	**TANGGUNGJAWAB**
Penolong Pengurus Pembangunan Aplikasi & Sistem adalah merupakan Pentadbir Sistem Aplikasi PAIP Berhad. 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 PKS PAIP Berhad; 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	PPPAS

tersebut diaktifkan penggunaannya; i. Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman virus dan penggodam ; j. Mematuhi dan melaksanakan prinsip-prinsip PKS dalam pengujudan akaun pengguna ke atas setiap sistem 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 ISMR jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;	

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020106 PENOLONG PENGURUS PEKHIDMATAN & SOKONGAN PENGGUNA(PSP)	**TANGGUNGJAWAB**
Penolong Pengurus Pekhidmatan & Sokongan Pengguna(PSP) adalah merupakan Pentadbir Teknikal dan Komunikasi ICT PAIP Berhad. Peranan dan tanggungjawab Pentadbir adalah seperti berikut : a. Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian Wireless PAIPNet 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 PAIPNet; e. Memantau penggunaan rangkaian dan melaporkan kepada ISMR sekiranya berlaku penyalahgunaan sumber rangkaian; f. Mewartakan polisi dan garis panduan penggunaan rangkaian PAIPNet kepada pengguna rangkaian; g. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian PAIPNet secara tidak sah;	PSP

h. Memastikan perisian antivirus dipasang pada aset ICT yang menggunakan rangkaian PAIPNet; dan i. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian	

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020107 PENTADBIR LAMAN WEB (WEBMASTER)	**TANGGUNGJAWAB**
Ketua Sub Unit Korporat adalah merupakan pentadbir laman web rasmi PAIP Berhad. Peranan dan tanggungjawab pentadbir laman web adalah seperti berikut: 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. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; e. Melaporkan sebarang pelanggaran keselamatan laman portal kepada ISMR. f. Mendapat kelulusan daripada Ketua Pegawai Eksekutif (CEO) sebelum disebarkan (kandungan laman web)	Ketua Sub Unit Korporat

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020108 PENTADBIR E-MEL	**TANGGUNGJAWAB**
Penolong Pengurus Sokongan Sistem, Infra & Teknologi Pekhidmatan & Sokongan Pengguna adalah merupakan pentadbir e-mel PAIP Berhad. 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 menghadapi tindakan tatatertib dengan arahan pengurusan atasan; c. Menyimpan jejak audit selama sekurang-kurangnya enam (6) bulan di dalam pelayan e-mel atau tertakluk kepada kemampuan ruang storan; d. Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; e. Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam; f. Memantau status storan e-mel pegawai & kakitangan PAIP Berhad dan memastikan sentiasa tersedia untuk transaksi e-mel; g. Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7;	PSP

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020108 PENTADBIR E-MEL	**TANGGUNGJAWAB**
h. Memastikan agar keupayaan *mail relay* hanya boleh digunakan untuk server atau aplikasi dalaman PAIP Berhad sahaja bagi tujuan keselamatan; i. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel PAIP Berhad; dan j. Memastikan pengguna e-mel PAIP Berhad berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel PAIP Berhad dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	PSP

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020109 PEGAWAI ASET ICT	**TANGGUNGJAWAB**
Pegawai Aset ICT di JPS adalah membantu Pegawai Aset PAIP Berhad bagi pengurusan aset ICT. Perlantikan ini dibuat oleh KJ. 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 PAIP Berhad dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c. Memastikan aset milik PAIP Berhad 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 f. Memastikan aset ICT yang ingin dilupuskan dilaksanakan mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	PAICT

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020110 PENGURUS PUSAT DATA DAN DISASTER RECOVERYCENTER (DRC)	**TANGGUNGJAWAB**
Pengurus adalah merupakan Pegawai yang menguruskan operasi Pusat Data dan *Disaster Recovery Center* (DRC) PAIP Berhad. Peranan dan tanggungjawab pegawai adalah seperti berikut : a. Memastikan Operasi Pusat Data dan DRC berada dalam keadaan baik sepanjang masa; b. Merancang dan menyelia pelaksanaan simulasi *Disaster Recovery Plan(DRP)* PAIP Berhad; c. Pengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data di PAIP Pekan; 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, *Unitrend, Tape Drive*) berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; f. Memantau aset ICT sokongan dan Fasiliti Sokongan (*Precision Aircond,* Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar sepanjang masa; g. Menguruskan permohonan baru dan pengemaskinian server dan *Virtual Machine* bagi sistem aplikasi baru di Pusat Data dan DRC	SSIT,PPAS, PSP

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.	SSIT,PPPAS, PSP

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020111 PENTADBIR STORAN AWAN (*CLOUD STORAGE*)	**TANGGUNGJAWAB**
Peranan dan tanggungjawab Pentadbir Storan Awan adalah : a. Menyelaras dan memastikan operasi sistem storan awan berada dalam keadaan baik sepanjang masa; b. Melakukan naik taraf kepada versi aplikasi storan awan yang digunakan; c. Melakukan *backup data* kepada storan awan yang disediakan; d. Melakukan integrasi kepada sebarang perisian operasi sistem pengguna dan jabatan serta sistem-sistem dalaman; e. Membuat konfigurasi dan penyelenggaraan berkala kepada perkakasan storan awan; f. Mendaftar dan membuat *housekeeping* kepada akaun pengguna storan awan; g. Memastikan saiz simpanan storan awan berada pada tahap yang optimum; h. Memastikan keselamatan kepada rangkaian dan data storan awan terjamin daripada serangan siber, bencana atau kerosakan; i. Menyediakan khidmat sokongan teknikal dan latihan kepada pengguna storan awan.	Pentadbir Storan Awan

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020112 MEJA BANTUAN ICT	**TANGGUNGJAWAB**
Peranan dan tanggungjawab Personel Meja Bantuan ICT adalah : a. Memberi bantuan segera kepada pengguna berkaitan masalah ICT yang dihadapi ; b. Perkhidmatan bantuan peringkat pertama bagi sebarang masalah ICT ; dan c. Mengagihkan isu dan masalah ICT kepada personel bertanggungjawab untuk penyelesaian.	Personel Meja Bantuan ICT

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020113 PENGGUNA	**TANGGUNGJAWAB**
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi PKS PAIP Berhad; b. Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya; c. Melepasi tapisan keselamatan; d. Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat PAIP Berhad; e. Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran , dan pemusnahan; dan vii. Menjaga kerahsiaan bagi setiap langkah-	Pengguna

langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ISMR dengan segera; g. Mengikuti dan menghayati serta menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. Menandatangani surat akuan pematuhan PKS PAIP Berhad sebagaimana **Lampiran 1**	

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
0201 INFRASTRUKTUR ORGANISASI KESELAMATAN	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS PAIP Berhad.	
020114 PASUKAN PAIP CERT	**TANGGUNGJAWAB**
Keanggotaan adalah seperti berikut: a. Pengarah CERT : CIO b. Pengurus CERT : ICTSO c. Ahli-ahli lain : i. SSIT (Operasi) ii. Ketua Sub Unit Korporat, (Portal) iii. PPAS (Pusat Data) PSP (Perkhidmatan & Sokongan Pengguna)Keahlian ini perlu mendapat kelulusan dari CIO PAIP Berhad. Laporan berkaitan keselamatan ICT akan dibentangkan secara tetap dalam Mesyuarat Jawatankuasa Pemandu ICT PAIP Berhad. Tanggungjawab Pasukan Pemandu ICT 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	PAIP CERT

	berlaku kepada ISMR 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.	

POLISI KESELAMATAN SIBER PAIP	
02 ORGANISASI KESELAMATAN	
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 PKS PAIP Berhad; 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 PAIP Berhad 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. PKS PAIP Berhad; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. Kod Tata Amalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Air)	Semua

f.	Menandatangani Surat Akuan Pematuhan Akta Rahsia Rasmi 1972 dan PKS PAIP Berhad sebagaimana **Lampiran 5.**	

POLISI KESELAMATAN SIBER PAIP	
03 KAWALAN DAN PENGELASAN ASET	
0301 AKAUNTABILITI ASET	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PAIP Berhad.	
030101 INVENTORI ASET	**TANGGUNGJAWAB**
Memastikan semua aset ICT PAIP Berhad 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 PAIP yang ditempatkan di PAIP Berhad ; d. Peraturan bagi pengendalian aset ICT PAIP hendaklah dikenalpasti, didokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT PAIP di bawah kawalannya.	Pegawai Aset ICT PAIP & Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
03 KAWALAN DAN PENGELASAN ASET	
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; b. Sulit; atau c. Terhad. Selain daripada maklumat terperingkat adalah dikelaskan sebagai terbuka.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
03 KAWALAN DAN PENGELASAN ASET	
0302 PENGELASAN DAN PENGENDALIAN MAKLUMAT	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
04 KESELAMATAN SUMBER MANUSIA	
0401 KESELAMATAN ICT DALAM TUGAS HARIAN	
Objektif : Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai, kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga PAIP Berhad 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 PAIP Berhad serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum , semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan PAIP Berhad serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selarasdengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma polisi – polisi dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

POLISI KESELAMATAN SIBER PAIP	
04 KESELAMATAN SUMBER MANUSIA	
0401 KESELAMATAN ICT DALAM TUGAS HARIAN	
Objektif : Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai, kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga PAIP Berhad hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
040102 DALAM PERKHIDMATAN	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan PAIP Berhad serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh PAIP Berhad; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT PAIP Berhad secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c. Memastikan adanya proses tindakan disiplin dan/atau undang- undang ke atas pegawai dan kakitangan PAIP Berhad sertapihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh PAIP Berhad; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan	Semua & Unit HRDC dan Latihan

keselamatan ICT. Sebarang kursus ICT umum yang diperlukan, pengguna boleh merujuk kepada Unit HRDC dan Latihan, Divisyen Pengurusan dan Sumber Manusia	

POLISI KESELAMATAN SIBER PAIP	
04 KESELAMATAN SUMBER MANUSIA	
0401 KESELAMATAN ICT DALAM TUGAS HARIAN	
Objektif : Untuk memastikan semua sumber manusia yang terlibat termasuk pegawai, kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga PAIP Berhad hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
040103 BERTUKAR ATAU TAMAT PERKHIDMATAN	**TANGGUNGJAWAB**
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT PAIP Berhad dikembalikan kepada PAIP Berhad mengikut peraturan dan/atau terma yang ditetapkan; b. Mengemaskini semua dokumentasi berkaitan pegawai dan kakitangan yang bertukar atau tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan PAIP Berhad; dan c. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh PAIP Berhad. d. Semua maklumat berkaitan PAIP Berhad hendaklah dihapuskan.	Semua

POLISI KESELAMATAN SIBER PAIP	
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 PAIP Berhad. 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 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	GM HR, ICTSO, Pegawai Aset dan Unit Aset dan Bangunan PAIP Berhad.

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.	

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0501 KESELAMATAN KAWASAN	
Objektif : Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050102 KAWALAN MASUK FIZIKAL	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap kakitangan PAIP Berhad hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan kembali kepada PAIP Berhad apabila kakitangan berhenti, bertukar atau bersara; c. Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di Lobi Utama PAIP Berhad atau Kaunter Pertanyaan (PAIP Daerah) terlebih dahulu dan hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas mestilah dilaporkan dengan segera kepada Unit Pentadbiran, Divisyen Pengurusan dan Sumber Manusia.	Semua Kakitangan & Pelawat & GM HR

POLISI KESELAMATAN SIBER PAIP

05 KESELAMATAN FIZIKAL

0501 KESELAMATAN KAWASAN

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

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 Pejabat PAIP Berhad adalah : a. Bilik Latihan ICT PAIP Berhad; b. Bilik Operasi Teknikal; c. Bilik-bilik pegawai PAIP Berhad; d. Stor Peralatan ICT; e. Pusat Data (Bilik Server) dan *Disaster Recovery Center* (DRC Pekan); f. Bilik Kawalan CCTV; dan g. Bilik Rak Rangkaian PAIPNet. 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 Kakitangan dan Penjaga bilik-bilik berkenaan

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
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 peralatan ICT 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 perisiantambahan tanpa kebenaran KJ; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus dikomputer peribadi atau komputer riba 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	Semua Kakitangan

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 KJ dan direkodkan bagi tujuan pemantauan;

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada KJ 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 KJ;

p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Helpdesk PAIP Berhad : **(https://helpdesk.paip.com.my)** 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 Kakitangan Teknikal 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 KJ. w. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya; dan x. Sebarang penggunaan peralatan ICT lain (bilik mesyuarat/latihan dan lain-lain) perlu mendapat kebenaran KJ.	

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050202 MEDIA MUDAH ALIH (*REMOVABLE MEDIA*)	**TANGGUNGJAWAB**
Media mudah alih merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetik, *DVDROM, pendrive* dan media storan lain. Media-media mudah alih perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada pengguna yang dibenarkan sahaja; c. Semua media mudah alih perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media mudah alih yang mengandungi data kritikal hendaklah disimpan di dalam **peti keselamatan** yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan media penyimpanan data; e. Akses dan pergerakan media mudah alih hendaklah direkodkan; f. Perkakasan *data backup* hendaklah diletakkan di tempat yang terkawal;	Semua Kakitangan

g. Mengadakan salinan atau penduaan (*backup*) pada media mudahalih kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Sebarang maklumat sulit dan rahsia yang disimpan di dalam media mudah alih perlulah dibuat enkripsi; i. Semua media mudah alih data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan j. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
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 KJ untuk tindakan seterusnya.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050204 MEDIA PERISIAN DAN APLIKASI	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pada peralatan ICT; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran KJ; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada DVDROM, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050205 MEDIA MUDAH ALIH PERSENDIRIAN (BRING YOUR OWN DEVICE)	**TANGGUNGJAWAB**
Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut: a. Semua peringkat maklumat rasmi PAIP Berhad adalah hakmilik PAIP Berhad; b. Sebarang bahan rasmi yang dimuatnaik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Pegawai Eksekutif (CEO); c. Menandatangani Surat Akuan Pematuhan PKS, Akta Rahsia Rasmi 1972 [Akta 88]. d. Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut: i. Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan; ii. Melaksanakan penyulitan dan/atau perlindungan ke atas *folder* yang mempunyai maklumat rasmi PAIP Berhad yang disimpan di dalam peranti BYOD; dan iii. Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti *antivirus, patching* terkini dan *anti theft*. e. Pengguna adalah dilarang daripada melakukan perkara berikut: i. Menyimpan maklumat rasmi di dalam BYOD tanpa kebenaran daripada KJ; ii. Menggunakan BYOD untuk mengakses,	Semua Kakitangan

menyimpan, dan menyebarkan maklumat rasmi dan terperingkat kepada pihak yang tidak dibenarkan tanpa kebenaran daripada KJ;

iii. Menjadikan BYOD sebagai medium sandaran (*backup*) bagi maklumat rasmi tanpa kebenaran daripada KJ;

iv. Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi tanpa kebenaran daripada KJ; dan

v. Menjadikan BYOD sebagai *access point* kepada aset ICT PAIP Berhad untuk capaian ke Internet tanpa kebenaran daripada KJ.

Pengguna adalah tertakluk kepada perkara seperti berikut:

a. Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa;

b. Memadamkan segala maklumat yang berkaitan dengan urusan rasmi PAIP Berhad sekiranya bertukar/ditamatkan perkhidmatan/bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan;

c. Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi PAIP Berhad;

d. PAIP Berhad berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan;

dan e. PAIP Berhad tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan untuk tujuan urusan rasmi PAIP Berhad.	

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050206 PENYELENGGARAAN PERKAKASAN	**TANGGUNGJAWAB**
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti perkakasan tersebut. 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 KJ.	Semua Kakitangan Teknikal IT

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050207 PEMINJAMAN ASET ICT BAGI KEGUNAAN DI LUAR PEJABAT	**TANGGUNGJAWAB**
Aset ICT yang dipinjam untuk kegunaan di luar pejabat PAIP Berhad adalah terdedah kepada pelbagai risiko. Aset ICT merangkumi peralatan, perisian, dan maklumat ICT. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan Aset ICT : a. Aset ICT yang dibawa keluar pejabat mestilah mendapat kelulusan KJ 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. f. Sebarang kerosakan semasa peminjaman aset ICT adalah tanggungjawab peminjam; dan g. Sebarang kehilangan semasa peminjaman aset ICT tersebut perlulah dilaporkan kepada pihak berkuasa dan kepada KJ.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0502 KESELAMATAN ASET ICT	
Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.	
050208 PENGENDALIAN PERALATAN LUAR YANG DIBAWA MASUK	**TANGGUNGJAWAB**
Bagi peralatan yang dibawa masuk ke premis PAIP Berhad, perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT PAIP Berhad; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh PAIP Berhad 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 PAIP Berhad. Jika ada, ia perlu disalin dan dihapuskan melainkan mendapat kebenaran daripada pegawai di tempat tugas dilaksanakan.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP

05 KESELAMATAN FIZIKAL

0502 KESELAMATAN ASET ICT

Objektif : Melindungi aset ICT dan maklumat daripada kehilangan, kerosakan, kecurian serta gangguan kepada aset ICT tersebut.

050209 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 PAIP Berhad dan ditempatkan di stor PAIP Berhad. 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 yangtelah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan	Pegawai Aset ICT

peralatan tersebut;

f. Pegawai aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Computerized Maintenance Management System (CMMS);

g. Pelupusan peralatan ICT PAIP Berhad 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 PAIP Berhad yang hendak dilupuskan tanpa kebenaran;

   iv. Melupuskan sendiri peralatan ICT PAIP Berhad kerana kerja-kerja pelupusan di bawah tanggungjawab PAIP Berhad; 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.

POLISI KESELAMATAN SIBER PAIP

05 KESELAMATAN FIZIKAL

0503 KESELAMATAN PERSEKITARAN

Objektif: Melindungi aset ICT Agensi dan Jabatan PAIP Berhad 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 Jabatan Pentadbiran PAIP Berhad. 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	Semua Kakitangan dan Unit Aset dan Jabatan Pentadbiran PAIP Berhad

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.	

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0503 KESELAMATAN PERSEKITARAN	
Objektif: Melindungi aset ICT Agensi dan Jabatan PAIP Berhad dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050302 BEKALAN KUASA	**TANGGUNGJAWAB**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepadaperalatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti 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.	JPS dan Unit Aset dan GM HR

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0503 KESELAMATAN PERSEKITARAN	
Objektif: Melindungi aset ICT Agensi dan Jabatan PAIP Berhad dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050303 KABEL TELEKOMUNIKASI DAN ELEKTRIK	**TANGGUNGJAWAB**
Kabel termasuk kabel elektrik atau telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. 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.	JPS

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0503 KESELAMATAN PERSEKITARAN	
Objektif: Melindungi aset ICT Agensi dan Jabatan PAIP Berhad dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
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 Pasukan Perhubungan Pusat Operasi Kecemasan (POK) PAIP Berhad yang dilantik.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
05 KESELAMATAN FIZIKAL	
0504 KESELAMATAN DOKUMEN	
Objektif: Melindungi maklumat Pejabat PAIP Berhad 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, atau Rahsia; 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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
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 diwujudkan, 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

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 PENGURUSAN PROSEDUR OPERASI	
Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan	
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 mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkoddan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 PENGURUSAN PROSEDUR OPERASI	
Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan	
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, menyelenggara, dan menguji aplikasi hendaklah dilaksanakan dalam persekitaran *development server* sebelum dimasukkan ke dalam *production server* yang menggunapakai persekitaran yang sama.	ICTSO

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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 kritikalsistem dan proses yang terlibat serta penilaian semula risiko.	Semua

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0602 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060201 PERKHIDMATAN PENYAMPAIAN	**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 & Pengurus Pusat Data dan DRC

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0603 PERANCANGAN DAN PENERIMAAN SISTEM	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 PENERIMAAN SISTEM	**TANGGUNGJAWAB**
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	PPPAS, Pentadbir Sistem Aplikasi

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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), *Content filtering* dan *Web Application Firewall (WAF)* 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 bagimemudahkan 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; 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	PSP

perisian berbahaya dan cara mengendalikannya; Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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 dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. d. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*;dan e. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan (*off-site*) dan selamat.	Pengurus Pusat Data dan DRC

POLISI KESELAMATAN SIBER PAIP 06 PENGURUSAN OPERASI DAN KOMUNIKASI 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 PAIPNet hendaklah melalui firewall di bawah kawalan Unit IT; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran KJ;	ICTSO, PSP

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 PAIPNet; i. Memasang *Web Content Filtering* untuk menyekat aktiviti *Web Surfing* yang dilarang semasa waktu kerja; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Unit IT adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian PAIPNet sahaja dan penggunaan rangkaian lain seperti 3G, 4G, HTE, LTE, ADSL dan *Wimax* adalah dilarang sama sekali kecuali telahmendapatkan kebenaran atas sebab tertentu dan penggunaannya perlulah di bawah seliaan serta pemantauan ketua divisyen/jabatan masing-masing; l. Sebarang penggunaan rangkaian komunikasi daripada agensi lain (contoh : PahangNet, 1GovNet) perlulah mendapat khidmat nasihat daripada ICTSO terlebih dahulu dan pelaksanaan secara berpusat perlulah menjadi keutamaan; dan m. Kemudahan rangkaian tanpa wayar (wireless) perlu dipantau dan dipastikan kawalan keselamatan.	

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0607 PENGURUSAN MEDIA	
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
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 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.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0607 PENGURUSAN MEDIA	
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
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. d. Mematuhi Akta-akta & Peraturan-peraturan yang sedia ada iaitu AR (Akta Rahsia), PDPA & KTA	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0608 PENGURUSAN PERTUKARAN MAKLUMAT	
Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara PAIP Berhad 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 PAIP Berhad dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari PAIP Berhad; dan d. Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0608 PENGURUSAN PERTUKARAN MAKLUMAT	
Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara PAIP Berhad dan agensi luar terjamin	
060802 PENGURUSAN MEL ELEKTRONIK (E-MEL)	**TANGGUNGJAWAB**
Penggunaan e-mel di PAIP Berhad hendaklah dipantau secara berterusan oleh Pentadbir e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam **garis panduan penggunaan e-mel rasmi Pengurusan Air Pahang Berhad** (PAIP Berhad) dan mana-mana undang-undang bertulis yang berkuat kuasa. Peraturan Penggunaan Emel Rasmi PAIP Berhad juga menjadi rujukan kepada kaedah pengurusan e-mel ini. Perkara-perkara yang perlu dipatuhi dalam pengendalian e-mel adalah seperti berikut : a. Akaun atau alamat e-mel yang diperuntukkan oleh PAIP Berhad 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 PAIP Berhad; 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 yangditetapkan agensi	Semua Kakitangan

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 disimpanmengikut 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.	

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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.	
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 c. Memastikan segala maklumat yang hendak dipaparkan telah disahkan serta diluluskan sebelum dimuat naik ke laman web	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
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 PAIP CERT : 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. Pasukan PAIP CERT akan menentukan prosedur pengumpulan bahan bukti (*hard disk*/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan	Semua Kakitangan

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.	

POLISI KESELAMATAN SIBER PAIP

06 PENGURUSAN OPERASI DAN KOMUNIKASI

0610 PEMANTAUAN

Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

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 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.	PPPAS,Pentadbir Sistem Aplikasi, KJPK, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, PSP

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0610 PEMANTAUAN	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061003 SISTEM LOG	**TANGGUNGJAWAB**
Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti 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, ICTSO hendaklah melaporkan kepada Pasukan PAIP CERT.	PPPAS,Pentadbir Sistem Aplikasi, KJPK, Pentadbir E-Mel, Pengurus Pusat Data dan DRC, PSP

POLISI KESELAMATAN SIBER PAIP	
06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0610 PEMANTAUAN	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
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 waktu yang dipersetujui.	PSP

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0701 KEPERLUAN KAWALAN CAPAIAN	
Objektif : Mengawal capaian ke atas maklumat dan kemudahan pemprosesan maklumat.	
070101 POLISI 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; d. Keselamatan maklumat yang dicapai menggunakan perkhidmatan storan awan; e. Kawalan ke atas kemudahan pemprosesan maklumat; f. Kawalan ke atas capaian aplikasi; dan g. Kawalan kebenaran untuk menyebarkan maklumat.	PSP

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0701 KEPERLUAN KAWALAN CAPAIAN	
Objektif : Mengawal capaian ke atas maklumat dan kemudahan pemprosesan maklumat.	
070102 KAWALAN CAPAIAN RANGKAIAN DAN PERKHIDMATAN RANGKAIAN	**TANGGUNGJAWAB**
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari PAIP Berhad. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b. Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian PAIP Berhad, rangkaian agensi lain dan rangkaian awam; dan c. Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar.	SSIT

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0701 KEPERLUAN KAWALAN CAPAIAN	
Objektif : Mengawal capaian ke atas maklumat dan kemudahan pemprosesan maklumat.	
070103 STORAN AWAN *(CLOUD STORAGE)*	**TANGGUNGJAWAB**
Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastuktur di pihak pengguna. Storan Awan (*Cloud storage*) adalah media penyimpanan dalam talian yang membolehkan pengguna menyimpan data/maklumat di server virtual (pelayan maya) yang tersedia. Dengan adanya *cloud storage*, pengguna tidak perlu lagi membawa storan fizikal. a. Penggunaan dan penyediaan perkhidmatan pemgkomputeran dan storan awan perlu mendapat kelulusan daripada pihak PAIP Berhad. Pengkomputeran awan yang digunakan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat.	SSIT

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0702 PENGURUSAN CAPAIAN PENGGUNA	
Objektif : Mengawal capaian pengguna ke atas aset ICT PAIP Berhad.	
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 PAIP Berhad sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi capaian minimum yang akan ditetapkan oleh pemilik sistem; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; 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 tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bersara atau Berhenti; atau iv) Ditamatkan perkhidmatan	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0702 PENGURUSAN CAPAIAN PENGGUNA	
Objektif : Mengawal capaian pengguna ke atas aset ICT PAIP Berhad.	
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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP

07 KAWALAN CAPAIAN

0702 PENGURUSAN CAPAIAN PENGGUNA

Objektif : Mengawal capaian pengguna ke atas aset ICT PAIP Berhad.

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 PAIP Berhad seperti berikut : a. Dalam apa juga 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 sepuluh (10) aksara dengan gabungan aksara, angka dan aksara khusus bagi Sistem Perolehan Berpusat (CPS) dan Webmail manakala kata laluan sistem-sistem yang lain mestilah sekurang – kurangnya enam (6) aksara; 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; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Menguatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula oleh sistem; h. Had cubaan kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah mengikut kesesuaian sistem. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

selama mengikut kesesuaian sistem atau setelah diset semula oleh Pentadbir Sistem Aplikasi; i. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; j. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0702 PENGURUSAN CAPAIAN PENGGUNA	
Objektif : Mengawal capaian pengguna ke atas aset ICT PAIP Berhad.	
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: 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.	Semua Kakitangan

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
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 peranti keselamatan yang bersesuaian di antara rangkaian PAIPNet, 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.	PSP

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0703 KAWALAN CAPAIAN RANGKAIAN	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070302 CAPAIAN INTERNET	**TANGGUNGJAWAB**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di dalam PAIPNet 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 PAIPNet; b. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Perkhidmatan dan Sokongan Pengguna berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya setelah mendapat maklumat dari KJ;	PSP

e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua divisyen/jabatan;

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 Ketua Divisyen/Jabatan sebelum dimuat naik ke Internet;

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

i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PAIP Berhad;

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 ruang kerja pejabat; dan

l. Pengguna adalah dilarang melakukan aktiviti-

aktiviti seperti berikut : • 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 • Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
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. Mewujudkanjejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *administrator*; 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 setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Mengehadkan dan mengawal penggunaan	Pegawai Aset ICT, PSP

program; dan d. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
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 menyebabkankerosakan. 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 atau mengikut kesesuaian sistem. 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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0706 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
07 KAWALAN CAPAIAN	
0707 KAWALAN CAPAIAN PERKHIDMATAN HOSTING	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem aplikasi yang hosting di Pusat Data.	
070701 CAPAIAN PERKHIDMATAN *HOSTING*	**TANGGUNGJAWAB**
Kawalan capaian perkhidmatan *Hosting* perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi *server* perlu digunakan bagi : a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b. Merekodkan capaian yang berjaya dan gagal; dan c. Menghadkan dan mengawal capaian aplikasi pengguna. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara- perkara berikut : a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkanjejak audit ke atas semua capaian sistem *hosting*; 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 *hosting* menggunakan prosedur log on yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c. Mengehadkan tempoh sambungan ke sesebuah aplikasi *hosting* berisiko tinggi; dan d. Memaklumkan sebarang perubahan atau	Pengurus Pusat Data dan DRC

pertukaran pengguna bagi tujuan pembatalan atau pewujudan kata laluan.	

POLISI KESELAMATAN SIBER PAIP	
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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
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.	
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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0802 KAWALAN KRIPTOGRAFI	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0802 KAWALAN KRIPTOGRAFI	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
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 Kakitangan

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0804 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080402 PEMBANGUNAN PERISIAN SECARA OUTSOURCE	**TANGGUNGJAWAB**
Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau olehpegawai yang dipertanggungjawabkan. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik PAIP Berhad.	Pentadbir Sistem Aplikasi, Pentadbir Laman Web, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0805 KAWALAN TEKNIKAL KETERDEDAHAN (VULNERABILITY)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 KAWALAN DARI ANCAMAN TEKNIKAL	**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, PSP (Pentadbir E-Mel), SSIT(Pengurus Pusat Data dan DRC, Pentadbir Storan Awan)

POLISI KESELAMATAN SIBER PAIP	
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 PKS sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada PAIP CERT dengan kadar segera : a. Maklumat didapati 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 didapati atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di PAIP Berhad sepertimana **Lampiran 2.** Prosedur pelaporan insiden keselamatan ICT berdasarkan : a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden	Semua

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* (PAIP CERT).	

POLISI KESELAMATAN SIBER PAIP

09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

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 yangtinggi kepada PAIP Berhad. 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 berkuatkuasa perundangan sekiranya perlu.	ICTSO, PAIP CERT

POLISI KESELAMATAN SIBER PAIP	
10 PENGURUSAN KESINAMBUNGANPERKHIDMATAN	
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 tersebutterhadap fungsi kritikal jabatan dan penentuan strategi bagi memastikan perkhidmatan jabatan tetap dapat diteruskan walaupun berlakugangguan/bencana. Pelan Kesinambungan Perkhidmatan (PKP) adalah pelan menyeluruh bagi menyedia dan memulihkan jabatan agar dapat meneruskan perkhidmatan dalam tempoh masa sesingkat mungkin semasa bencana atau gangguan. Selain PKP, Pelan Pemulihan Bencana (DRP) juga dirujuk sebagai prosedur untuk kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh PAIP CERT 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	CIO,ICTSO,SSIT

ditetapkan;

d. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
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 PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut :

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b. Senarai personel PAIP Berhad 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 PKP perlu disimpan di lokasi berasingan

untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan PKP 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 PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.PAIP Berhad hendaklah memastikan salinan pelan PKP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

POLISI KESELAMATAN SIBER PAIP	
11 PEMATUHAN	
1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS PAIP Berhad	
110101 PEMATUHAN POLISI	**TANGGUNGJAWAB**
Setiap pengguna di PAIP Berhad hendaklah membaca, memahami dan mematuhi PKS PAIP Berhad dan peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di PAIP Berhad termasuk maklumat yang disimpandi dalamnya adalah hak milik PAIP Berhad dan Pengurus Besar/Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT PAIP Berhad selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber PAIP Berhad.	Semua

POLISI KESELAMATAN SIBER PAIP	
11 PEMATUHAN	
1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS PAIP Berhad	
110102 PEMATUHAN DENGAN DASAR, PIAWAIAN DAN KEPERLUAN TEKNIKAL	**TANGGUNGJAWAB**
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

POLISI KESELAMATAN SIBER PAIP	
11 PEMATUHAN	
1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS PAIP Berhad	
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 kebarangkalianberlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

POLISI KESELAMATAN SIBER PAIP	
11 PEMATUHAN	
1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS PAIP Berhad	
110104 KEPERLUAN PERUNDANGAN	**TANGGUNGJAWAB**
Senarai perundangan dan peraturan yang perlu dipatuhi oleh pengguna di PAIP Berhad adalah seperti di **Lampiran 3**.	Semua

POLISI KESELAMATAN SIBER PAIP	
11 PEMATUHAN	
1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS PAIP Berhad	
110105 PERLANGGARAN POLISI	**TANGGUNGJAWAB**
Pelanggaran PKS PAIP Berhad boleh dikenakantindakan tatatertib.	Semua

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 jangka masa yang ditetapkan.
Cloud Computing	Cloud Computing adalah perkhidmatan sumber-sumber ICT yang dimayakantanpa penyediaan infrastuktur di pihak pengguna.
Cloud Storage	Cloud Storage adalah perkhidmatan media penyimpanan dalam talian yang membolehkan pengguna menyimpan data/maklumat di server virtual (pelayan maya).
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidakdifahami 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 bentukperkakasan 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).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebihpantas.

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.
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 satutrafik 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 maliciouscode. 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.
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 (PKI) 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
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.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

PENGURUSAN AIR PAHANG BERHAD (200801004468)

LAMPIRAN 1

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Lokasi : .....

Divisyen/Jabatan/Unit/ : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : .....

Tarikh : .....

Rujukan:

Sila layari
POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD
http://www.paip.com.my/

LAMPIRAN 2

SECURITY BREACHES/INCIDENT & RESPONSE LOG
(PAIP-SR-F01)

LAMPIRAN 3

SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan;
2. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan TeknologiMaklumat dan Komunikasi (ICT);
3. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
4. Akta Tandatangan Digital 1997;
5. Akta Rahsia Rasmi 1972;
6. Akta Hak Cipta (Pindaan) Tahun 1997;
7. Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT *Computer Emergency Response Team* (PAIP CERT).
8. Kod Tata Amalan (Perlindungan Data Peribadi Untuk Sektor Utiliti (Air)

LAMPIRAN 4

SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

PERAKUAN UNTUK DITANDATANGANI BERKENAAN DENGAN AKTA RAHSIA RASMI 1972 DAN POLISI KESELAMATAN SIBER PENGURUSAN AIR PAHANG BERHAD

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 Pengurusan Air Pahang Berhad 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 Pengurusan air Pahang Berhad terkini berkenaan Perkara : Keperluan Keselamatan Kontrak dengan Pihak Ketiga dan mematuhi Akta-Akta yang ada di dalam Lampiran 3. Selain itu, saya juga telah membaca dan faham serta akan mematuhi polisi lain di dalam Polisi Keselamatan Siber Pengurusan Air Pahang Berhad 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 Pengurusan Air Pahang Berhad seperti semua keterangan perenggan di atas. Oleh itu, sesiapa yang tiada dalam senarai **Lampiran A** tersebut tidakdibenarkan 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 :**
Tarikh :	**Tarikh :**

LAMPIRAN A

SENARAI KAKITANGAN SYARIKAT YANG TERLIBAT DALAM URUSAN BERKAITAN .....

DENGAN PENGURUSAN AIR PAHANG BERHAD.

BIL.	NAMA & DIVISYEN / JABATAN / UNIT / SYARIKAT	JAWATAN	NO KAD PENGENALAN

***Sila lengkapkan dengan tulisan HURUF BESAR**