PELAN PENGURUSAN KESELAMATAN MAKLUMAT

PEJABAT SETIAUSAHA KERAJAAN
NEGERI PULAU PINANG

VERSI 1.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
13 Ogos 2019	1.0	Mesyuarat JKP eGG Bil. 2/2019	1 September 2019

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN

Pelan Pengurusan Keselamatan Maklumat versi 1.0 ini dipanjangkan kepada semua Pejabat Setiausaha Kerajaan Negeri untuk diterima pakai manakala Agensi Negeri dan Pihak Berkuasa Tempatan Negeri adalah tertakluk kepada penerimaan oleh pihak berkuasa masing-masing.

(DATO' ABDUL RAZAK BIN JAAFAR)

Setiausaha Kerajaan Negeri
Pulau Pinang

Kandungan

I. RINGKASAN EKSEKUTIF

Semakin banyak maklumat disimpan dalam bentuk digital di ruang siber, semakin mendesak satu rangka kerja keselamatan siber diperlukan bagi menangani amalan semasa pendekatan keselamatan siber secara silo.

Rangka kerja keselamatan siber ini memberi perspektif umum semua komponen keselamatan siber yang perlu diambil kira oleh Kerajaan Negeri dalam melindungi maklumat di ruang siber.

Rangka kerja ini dibangunkan berdasarkan rangka kerja keselamatan siber yang khusus bagi kementerian dan agensi Sektor Awam Malaysia.

Lapan (8) komponen utama rangka kerja keselamatan siber ini dan objektif komponen-komponen adalah seperti berikut :

(i) **Kenal Pasti** yang bertujuan mengenal pasti persekitaran fungsi PSUKPP, polisi dan struktur tadbir urus serta aset yang perlu dilindungi, risiko berkaitan dan pengurusan risiko;

(ii) **Lindung** memerlukan prinsip-prinsip keselamatan, teknologi, proses dan kompetensi manusia ditentukan bagi memitigasi risiko-risiko yang telah dikenal pasti;

(iii) **Kesan** membawa objektif untuk mengesan ancaman kod jahat dengan menekankan kepada kelainan dalam penggunaan dan bentuk trafik rangkaian;

(iv) **Tindak Balas** sebaliknya pula memastikan tindakan terhadap ancaman kod jahat ini diambil dan dilaporkan kepada pemegang taroh dan orang awam (jika diperlukan);

(v) **Pulih** mengambil kira keupayaan dalam memastikan ketersediaan maklumat, akan melaksanakan pemulihan akibat kerosakan yang berpunca daripada ancaman kod jahat dan kegagalan sistem;

(vi) **Peroleh** adalah untuk memastikan kawalan keselamatan dan keperluan-keperluan yang dikuatkuasakan dalam keseluruhan kitar hayat sistem baik bagi perolehan luaran mahu pun perolehan bagi pembangunan secara dalaman. Komponen ini merupakan komponen penting yang meliputi spesifikasi perolehan, pengurusan syarikat pembekal, jejak sumber, kitar hayat pembangunan sistem, pentauliahan dan pelucutan pentauliahan serta pelupusan sistem;

(vii) **Audit Keselamatan** dan

(viii) **Kuat Kuasa** merentasi semua komponen bagi mengariskan skop audit dan penguatkuasaan yang dilaksanakan oleh agensi audit dan pihak berkuasa penguatkuasaan.

II. PENGENALAN

Salah satu langkah dalam transformasi Sektor Awam di Malaysia adalah penggunaan ICT untuk meningkatkan kecekapan dalam Penyampaian Perkhidmatan Kerajaan. Ini bermakna maklumat atau data disimpan dan diproses dalam bentuk digital, atau dalam erti kata lain, dalam ruang siber.

Sehubungan dengan itu, suatu Pelan Pengurusan Keselamatan Maklumat menyeluruh diperlukan bagi Kerajaan Negeri bertujuan memberi panduan asas serta merangkumi kesemua komponen keselamatan yang perlu diambil kira untuk melindungi maklumat dalam ruang siber mereka.

III. SKOP

Dokumen ini Pelan Pengurusan Keselamatan Maklumat yang mesti digunakan oleh Kerajaan Negeri dalam merancang perlindungan yang diperlukan bagi ruang siber masing-masing.

Dalam konteks dokumen ini**, ruang siber ditakrifkan sebagai sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan.**

Maklumat yang dipindahkan dari ruang siber ke ruang fizikal (melalui cetakan, salinan tulisan tangan, rakaman foto menggunakan peralatan fotografik) adalah di luar skop dokumen ini dan hendaklah ditangani dengan peraturan sedia ada.

IV. SINGKATAN DAN TAKRIFAN

1. Singkatan

a)	**PKP**	Pengurusan Kesinambungan Perkhidmatan
b)	**CGSO**	Chief Government Security Office / Pejabat Ketua Pegawai Keselamatan Kerajaan
c)	**DRC**	Disaster Recovery Centre / Pusat Pemulihan Bencana
d)	**ICT**	Information Communication and Technology / Teknologi Maklumat dan Komunikasi
e)	**ICTSO**	ICT Security Officer / Pegawai Keselamatan ICT
f)	**ISMS**	Information Security Management System / Sistem Pengurusan Keselamatan Maklumat
g)	**MAMPU**	Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
h)	**PDRM**	Polis Diraja Malaysia
i)	**PII**	Maklumat Pengecaman Individu
j)	**SKMM**	Suruhanjaya Komunikasi Dan Multimedia Malaysia
k)	**PSUKPP**	Pejabat Setiausaha Kerajaan Negeri Pulau Pinang
l)	**Bring Your Own Device (BYOD)**	Garis panduan ini disediakan untuk menggariskan satu tatacara penggunaan secara selamat semua peranti mudah alih supaya selaras dengan prinsip Confidentiality, Integrity dan Availability (CIA).
m)	**Central Processing Unit (CPU)**	Unit Pemprosesan Utama iaitu yang mengandungi processor, hard disk, memori dan papan utama.
n)	**Computer Emergency Response Team (CERT)**	Pasukan yang akan bertindak sekiranya berlaku bencana atau perkara-perkara yang tidak diingini.
o)	**Hub**	Peralatan rangkaian menghubung satu stesen kerja dengan stesen kerja yang lain.
p)	**Intrusion Detection Sistem (IDS)**	Satu peralatan yang digunakan untuk memantau atau merekod cubaan pencerobohan.

q)	**Internet**	Perkhidmatan informasi secara global yang menghubungkan semua pengguna seluruh dunia melalui satu protokol rangkaian.
r)	**Information Security**	Proses dan mekanisme untuk melindungi maklumat.
s)	**Jawatankuasa Pemandu *Electronic Good Governance (eGG)***	Jawatankuasa ICT Tertinggi di peringkat Kerajaan Negeri Pulau Pinang yang diketuai oleh Setiausaha Kerajaan Negeri dan dianggotai oleh semua Ketua-ketua Jabatan di setiap Jabatan/ Agensi Negeri.
t)	**Ketua Pegawai Maklumat (CIO)**	Pegawai yang dilantik dan bertanggungjawab dalam perancangan dan pembangunan ICT sesebuah agensi kerajaan.
u)	**Kriptografi**	Kaedah untuk menukar maklumat biasa kepada format yang tidak boleh difahami.
v)	**Pegawai Keselamatan ICT (ICTSO)**	Pegawai yang bertanggungjawab untuk menjaga keseluruhan keselamatan maklumat.

2. Takrifan

a) **PSUKPP** merujuk kepada Kementerian, Pejabat Kerajaan, Badan Berkanun, Kerajaan Tempatan dan lain-lain agensi.

b) **Keselamatan Siber** merujuk kepada koleksi alat, dasar, konsep keselamatan, perlindungan keselamatan, garis panduan, pendekatan pengurusan risiko, tindakan, latihan, amalan terbaik, jaminan dan teknologi yang boleh digunakan untuk melindungi alam siber agensi dan aset pengguna. Agensi dan aset pengguna termasuk peranti komputer yang disambungkan, kakitangan, infrastruktur, aplikasi, perkhidmatan, sistem telekomunikasi, dan keseluruhan maklumat yang dihantar dan / atau disimpan di dalam persekitaran siber. Keselamatan Siber usaha untuk memastikan pencapaian dan penyelenggaraan ciri-ciri keselamatan organisasi dan aset pengguna terhadap risiko keselamatan yang relevan dalam persekitaran siber. Objektif keselamatan umum adalah seperti berikut:

(i) Ketersediaan

(ii) Integriti, yang mungkin termasuk kesahihan dan bukan penolakan

(iii) Kerahsiaan

c) **Produk Kriptografi Terpercaya** merujuk kepada produk kriptografi yang dinilai dan di iktiraf oleh Kerajaan bertujuan untuk mengawal dan menjaga keselamatan maklumat, integriti, pengesahan dan tidak boleh di sangkal.

V. TATACARA PENGGUNAAN DOKUMEN

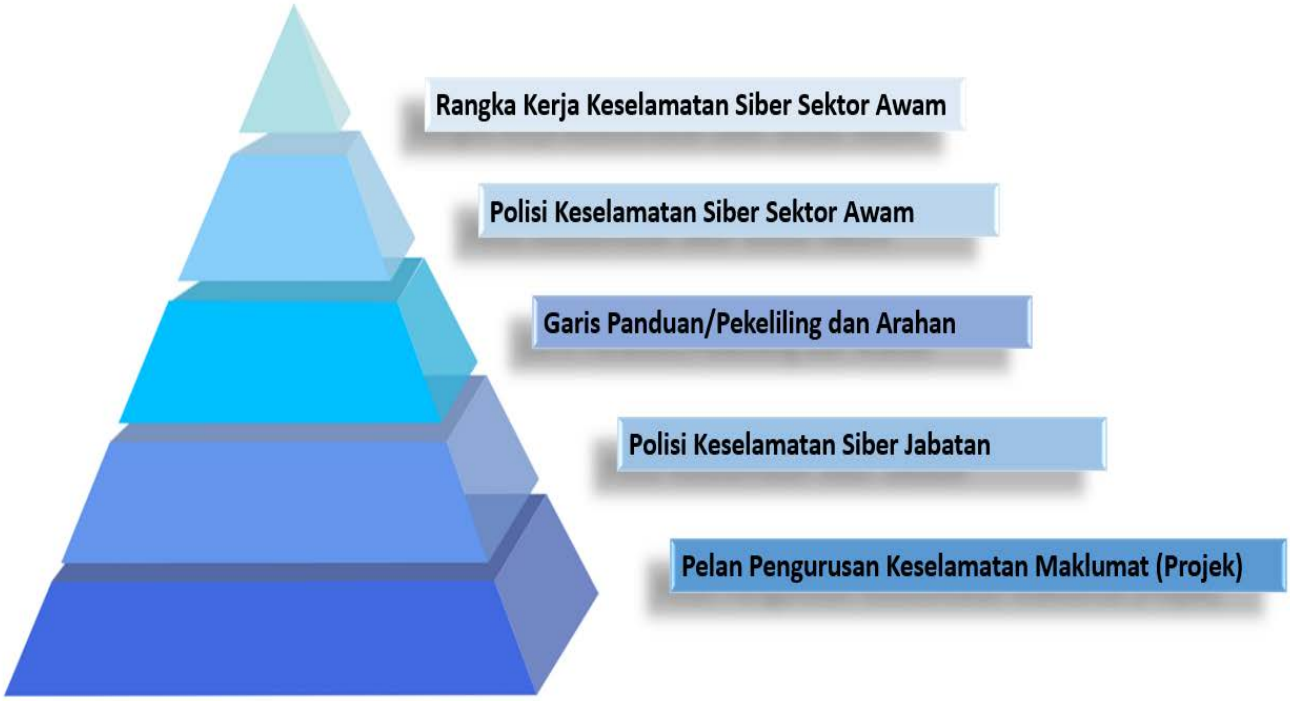
Di peringkat projek, dokumen ini hendaklah dirujuk untuk merangka Pelan Pengurusan Keselamatan Maklumat. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat mengikut struktur rangka kerja yang terdapat dalam dokumen ini. Pelan Pengurusan Keselamatan Maklumat akan disemak semula secara tahunan atau mengikut keperluan.

Kawalan tambahan boleh dibangunkan dan diguna pakai untuk mengambil kira keperluan tahap keselamatan yang lebih tinggi bagi sektor tertentu seperti penguatkuasaan undang-undang, keselamatan nasional.

Dokumen tambahan boleh dibangunkan oleh Kerajaan untuk memperincikan aspek tertentu dalam rangka kerja ini.

Agensi pengauditan boleh menggunakan dokumen ini untuk memastikan Pelan Pengurusan Keselamatan Maklumat bagi pelaksanaan sistem ICT adalah lengkap dan menentukan tahap keselamatan dan kematangan sistem.

Rajah 1 menerangkan kepada agensi-agensi Sektor Awam berkenaan hirarki dokumen yang perlu dirujuk bagi merancang perlindungan keselamatan siber.



Rajah 1 : Hirarki Rujukan Dokumen

Terdapat tiga (3) peringkat dalam pembangunan polisi keselamatan siber. Peringkat teratas adalah halatuju polisi umum melalui Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan Polisi Keselamatan Siber Sektor Awam. Peringkat seterusnya adalah Dasar Keselamatan ICT Negeri Pulau Pinang yang memberi perhatian kepada isu-isu khusus PSUKPP.

Pelan Pengurusan Keselamatan Maklumat dengan berpandukan RAKKSSA, Dasar Keselamatan ICT Negeri Pulau Pinang dan surat pekeliling/arahan terkini, dibangunkan untuk menangani isu-isu operasi projek.

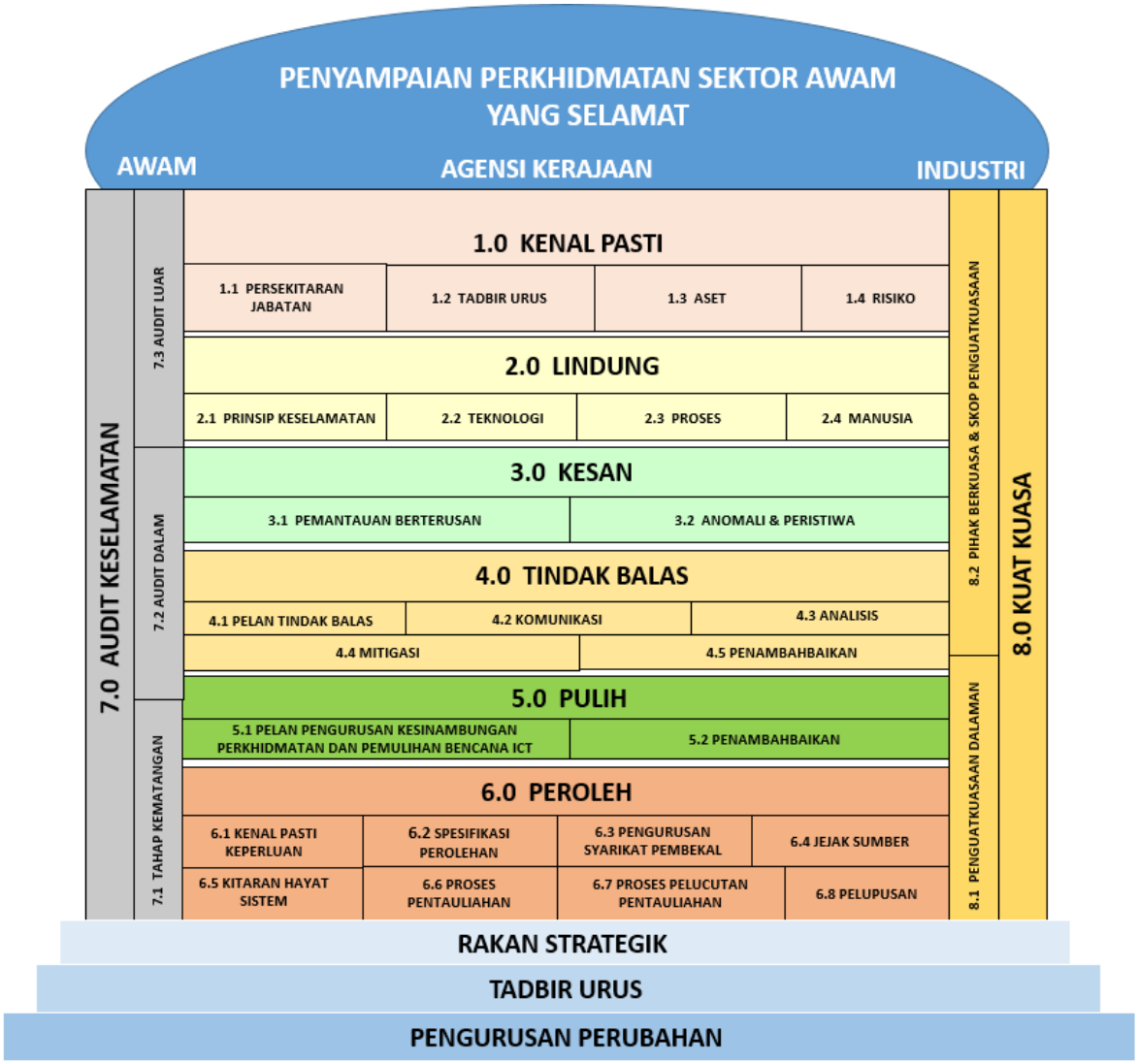
Polisi di peringkat pusat adalah bersifat umum dan tidak berubah dalam jangka masa pendek. Manakala polisi di peringkat PSUKPP perlu disemak dengan lebih kerap mengikut perubahan teknologi, permintaan, keperluan, undang-undang dan fungsi PSUKPP.

Pelan Pengurusan Keselamatan Maklumat bagi projek mengandungi maklumat terperinci, menyatakan keutamaan aplikasi, kawalan capaian dan lain-lain keperluan khusus.

VI. GAMBARAN KESELURUHAN RANGKA KERJA KESELAMATAN SIBER SEKTOR AWAM

Objektif RAKKSSA adalah bagi memastikan keselamatan penyampaian perkhidmatan Sektor Awam sekaligus meningkatkan tahap keyakinan kepada pihak berkepentingan (agensi Kerajaan, industri dan orang awam)..

RAKKSSA terdiri daripada lapan (8) komponen utama seperti yang digambarkan dalam Rajah 2.



Rajah 2: Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

Lapan (8) komponen utama RAKKSSA adalah seperti yang berikut :

Komponen	Objektif
Kenal Pasti	Mengenal pasti persekitaran fungsi PSUKPP, polisi dan struktur tadbir urus serta aset yang perlu dilindungi, risiko berkaitan dan pengurusan risiko.
Lindung	Menentukan prinsip-prinsip keselamatan, kompetensi manusia, proses dan teknologi yang diperlukan bagi bagi memitigasi risiko-risiko yang telah dikenal pasti. Kompetensi manusia merupakan faktor penentu penggunaan teknologi yang betul dan mematuhi proses.
Kesan	Mengesan ancaman serangan berniat jahat dengan menekankan kepada anomali dalam penggunaan dan corak trafik rangkaian. Ini termasuk pemantauan berterusan dan penentuan maklumat asas.
Tindak Balas	Bertindak balas kepada serangan berniat jahat semasa dan selepas kejadian. Ini termasuk menyalurkan maklumat kepada pemegang taroh dan makluman kepada orang awam.
Pulih	Melaksanakan tindakan pemulihan terhadap kerosakan yang disebabkan oleh serangan berniat jahat dan kegagalan sistem untuk memastikan ketersediaan data.
Peroleh	Memastikan keperluan dan langkah-langkah keselamatan dilaksanakan pada setiap peringkat kitar hayat sistem. Ini termasuk spesifikasi perolehan, pengurusan syarikat pembekal, jejak sumber, kitar hayat pembangunan sistem, proses pentauliahan dan pelucutan pentauliahan sehingga sistem pelupusan. Perolehan sistem boleh merupakan pembangunan secara luaran atau dibangunkan secara dalaman.
Audit Keselamatan	Menggariskan skop audit dan pihak berkuasa audit.
Kuat Kuasa	Menggariskan skop penguatkuasaan dan pihak berkuasa penguatkuasaan.

PSUKPP menggunakan rangka kerja ini bagi membangunkan Pelan Pengurusan Keselamatan Maklumat mengikut susunan dokumen ini. Audit Keselamatan dan Kuat Kuasa merupakan dua komponen yang merentasi semua komponen.

1.0 KENAL PASTI

Langkah pertama dalam perancangan keselamatan siber adalah mengenal pasti persekitaran fungsi dan perkhidmatan Pejabat Setiausaha Kerajaan Negeri Pulau Pinang (PSUKPP), struktur tadbir urus dan aset dalam skop perlindungan.

Langkah seterusnya adalah untuk mengenal pasti ancaman ke atas aset atau persekitaran fungsi dan perkhidmatan PSUKPP.

Risiko merupakan kebarangkalian dan impak sesuatu insiden berlaku berpunca daripada kerentanan dan ancaman yang dikenal pasti. Kerajaan Negeri hendaklah mengenal pasti peranan dan tanggungjawab pemilik aset dan pemilik risiko dalam struktur tadbir urus. Pemilik risiko hendaklah memastikan pengolahan risiko merangkumi proses, teknologi dan manusia.

1.1 Persekitaran Perkhidmatan dan Fungsi PSUKPP

Pelan Pengurusan Keselamatan Maklumat adalah meliputi persekitaran perkhidmatan dan Pelan Hala Tuju PSUKPP.

1.1.1 Peranan PSUKPP

Pelan Strategik PSUKPP telah disediakan sebagai panduan dan hala tuju PSUKPP dalam melaksanakan program dan aktiviti ICT yang berkaitan.

1.1.2 Kebergantungan PSUKPP

Kebergantungan sumber maklumat diperolehi daripada kerjasama dan ketersediaan maklumat antara PSUKPP, PSUKPP dan agensi negeri.

Maklumat tersebut perlu dikelaskan mengikut tahap kerahsiaan yang ditetapkan oleh pemegang taroh.

1.2 Tadbir Urus

PSUKPP telah mewujudkan tadbir urus untuk pengurusan keselamatan maklumat iaitu Computer Emergency Response Team (CERT) Negeri Pulau Pinang. Skop dan tanggungjawab CERT Negeri Pulau Pinang adalah seperti yang digariskan dalam Dasar Keselamatan ICT Negeri Pulau Pinang.

1.2.1 Keperluan Perundangan dan Peraturan

PSUKPP mematuhi perundangan, peraturan, polisi dan garis panduan yang telah diwartakan oleh Kerajaan. Dasar Keselamatan Teknologi Maklumat & Komunikasi (DKICT) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) PSUKPP yang merangkumi 14 bidang.

1.2.3 Garis Panduan Keselamatan Dasar Keselamatan Teknologi Maklumat & Komunikasi (DKICT)

PSUKPP telah membangunkan DKICT berdasarkan garis panduan yang sedang berkuat kuasa. Pematuhan kepada dasar keselamatan adalah mandatori. DKICT ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

1.3 Aset

1.3.1 Kategori Maklumat

Prosedur mengklasifikasikan maklumat yang diuruskan melalui aset ICT hendaklah berpandukan kepada Arahan Keselamatan Kerajaan seperti berikut :

a. Rahsia Besar;
b. Rahsia;
c. Sulit; atau Terhad.

1.3.1.1 Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu.

Sebaliknya, PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

1.3.1.2 Data Terbuka

Pelaksanaan perkongsian data dan data terbuka agensi Kerajaan Negeri hendaklah berpandukan Polisi Data Negeri Pulau Pinang.

1.3.2 Aliran Data

Aliran data dan komunikasi dalam PSUKPP perlu dikenal pasti dan direkodkan.

1.3.3 Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala seperti yang digariskan dalam MSISO Pembangunan Sistem Aplikasi.

1.3.4 Peranti Fizikal

Pengurusan aset ICT di PSUKPP perlu diuruskan seperti yang digariskan dalam DKICT, manakala pengurusan aset bagi peranti mudah alih perlu mematuhi Garis Panduan Bring Your Own Device (BYOD).

1.3.5 Sistem Luaran

Sistem luaran adalah sistem bukan milik PSUKPP yang digunakan dalam persekitaran PSUKPP. Sebagai contoh, sistem yang dikendalikan oleh organisasi awam yang memberi atau menerima maklumat.

1.3.6 Sumber Luaran

Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi PSUKPP. Contoh perkhidmatan sumber luaran ialah:

1.3.6.1. Perisian Sebagai Satu Perkhidmatan

1.3.6.2. Platform Sebagai Satu Perkhidmatan

1.3.6.3. Infrastruktur Sebagai Satu Perkhidmatan

1.3.6.4. Storan Pengkomputeran Awan

1.3.6.5. Pemantauan Keselamatan

1.4 Risiko

PSUKPP melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT seperti yang telah digariskan dalam DKICT.

1.4.1 Pengurusan Risiko

Sebarang insiden keselamatan ICT yang dikendalikan oleh CERT Negeri Pulau Pianng akan dibentangkan di Mesyuarat Jawatankuasa Pemandu electronic Good Governance (eGG). Pengurusan pengendalian insiden ini diuruskan sepenuhnya berdasarkan Prosedur Pengendalian Insiden Keselamatan ICT .

2.0 LINDUNG

Bahagian ini menyediakan mekanisme perlindungan yang diperlukan yang meliputi prinsip, teknologi, proses dan manusia.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi semua faktor dalam seksyen ini berdasarkan penilaian risiko dan pelan pengurusan risiko.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat yang berikut:

2.1 Prinsip Keselamatan

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori data yang dikendalikan oleh sistem.

Objektif utama keselamatan maklumat adalah:

- Kerahsiaan
- Integriti
- Ketersediaan
- Tanpa Sangkalan
- Pengesahan

Bagi mencapai objektif tersebut, PSUKPP melaksanakan prinsip keselamatan seperti berikut:

2.1.1 Prinsip “Perlu-Tahu”

PSUKPP hendaklah melaksanakan mekanisme bagi memberi kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang memberikan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi dan status bekerja pengguna tersebut.

2.1.2 Hak Keistimewaan Minimum

Pengguna hendaklah diberikan hak keistimewaan minimum untuk menjalankan tugasnya.

2.1.3 Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang, PSUKPP hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

2.1.4 Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

2.1.5 Peminimuman Data

PSUKPP hendaklah mengamalkan prinsip peminimuman data yang menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

2.2 Teknologi

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data dan pada setiap elemen pengkomputeran.

2.2.1 Peringkat Pemprosesan Data

2.2.1.1 Data dalam simpanan

PSUKPP menggunakan teknologi yang bersesuaian untuk melindungi data dalam simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data.

2.2.1.2 Data dalam pergerakan dan penggunaan

PSUKPP menggunakan teknologi yang bersesuaian untuk melindungi data dalam pergerakan dan penggunaan bagi menghalang capaian data yang tidak dibenarkan, memelihara integriti data serta menghadkan akses kepada kemudahan pemprosesan data atau maklumat seperti yang telah digariskan dalam DKICT.

2.2.1.3 Data-dalam-penggunaan

Teknologi yang bersesuaian untuk melindungi data dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan. Teknologi untuk memastikan asal data dan data/transaksi tanpa-sangkal boleh digunakan

2.2.1.4 Perlindungan Ketirisan Data

Melaksanakan akses atas dasar perlu mengetahui terhadap penggunaan aset dan sistem aplikasi ICT.

2.2.2 Elemen Dalam Persekitaran Pengkomputeran

Bagi memastikan tahap keselamatan ICT Kerajaan Negeri sentiasa pada tahap yang tinggi dalam menghadapi sebarang ancaman keselamatan ICT , PSUKPP melaksanakan perkara -perkara seperti di **Lampiran 1**.

2.2.2.3 Aplikasi

Perisian aplikasi digunakan untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi adalah pelayan web, pelayan aplikasi dan sistem operasi.

Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

Bagi memastikan kawalan capaian sistem maklumat dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:

2.2.3.1. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi mengikut tahap capaian yang dibenarkan dan sensitiviti maklumat yang telah ditentukan;

2.2.3.2. Memaparkan notis amaran pada skrin pengguna sebelum pengguna memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;

2.2.3.3. Menghadkan capaian kepada 3 kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;

2.2.3.4. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelak aktiviti dan capaian yang tidak sah; dan

2.2.3.5. Sistem yang sensitif perlu diasingkan.

2.2.2.4 Pelayan

Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

2.2.2.5 Persekitaran Fizikal

Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT iaitu Pusat Data Utama dan Pusat DRC. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

2.2.3 Kawalan Capaian

2.2.3.1 Fizikal

PSUKPP hendaklah melaksanakan kawalan akses ke atas Kawasan Terperingkat. Pengesahan pengguna bagi kemasukan ke lokasi fizikal adalah berdasarkan pengenalan fizikal termasuk dokumen fizikal,pembaca biometrik,atau pembaca jarak dekat, atau pembaca PIN atau gabungan teknologi di atas.

2.2.3.2 Pengenalan Pengguna

Pengenalan pengguna hendaklah merujuk kepada seseorang pengguna sahaja. Pengeluaran pengenalan pengguna kepada kakitangan Sektor Awam hendaklah tertakluk kepada proses pengesahan yang ketat.

Pengenalan pengguna digunakan oleh kakitangan Sektor Awam bagi tujuan pengesahan diri untuk menggunakan aplikasi.

2.2.3.3 Pengesahan Pengguna

Pengesahan pengguna kepada aplikasi PSUKPP hendaklah berdasarkan pengenalan pengguna yang diiktiraf oleh pihak berkuasa.

Semua aplikasi PSUKPP menggunakan fungsi Single Sign-On.

2.2.3.4 Kebenaran Pengguna

Setelah seseorang pengguna disahkan, sistem hendaklah menentu dan memberikan akses yang dibenarkan kepada pengguna tersebut. Bagi memastikan sistem maklumat dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.

Pemilikan akaun pengguna bukanlah hak mutlak seseorang. la merupakan kemudahan yang tertakluk kepada peraturan PSUKPP dan boleh ditarik balik jika penggunaannya melanggar peraturan. Langkah-langkah berikut hendaklah dipatuhi:

a. Jangan dedahkan kata laluan. Pengguna hendaklah merahsiakan kata laluan dari pengetahuan orang lain;

b. Pengguna diminta menukar kata laluan setiap satu tahun sekali bagi mengelak akaun mudah dicerobohi;

c. Pengguna hendaklah menggunakan kata laluan yang sukar diteka, sekurang-kurangnya lapan (12) aksara dengan gabungan alphanumeric dan simbol khas;

d. Pengguna adalah dilarang melakukan pencerobohan ke atas akaun pengguna lain. Perkongsian akaun juga adalah dilarang; dan

Pemberian kata laluan perlu dikawal melalui satu proses pengurusan yang formal. Semakan kepada kebenaran capaian pengguna dikaji setiap tahun (jika ada keperluan).

2.2.4 Kriptografi

Perkara-perkara berkaitan penyulitan maklumat perlu diuruskan berdasarkan kawalan penyulitan maklumat dan polisi penggunaan penyulitan maklumat seperti yang telah digariskan dalam DKICT.

2.2.5 Rangkaian

Pengurusan Keselamatan Rangkaian perlu dilaksanakan seperti yang telah digariskan dalam DKICT.

2.3 Proses

2.3.1 Konfigurasi Asas

Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi pra-syarat pentauliahan sistem.

Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

2.3.2 Kawalan Perubahan Konfigurasi

Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan difaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

Pengubahsuaian mestilah mendapat kebenaran pihak pengurusan atau pemilik aset ICT terlebih dahulu.

Aktiviti-aktiviti seperti pemasangan, penyelenggaraan, mengemas kini komponen aset dan sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa

dan mempunyai pengetahuan dan kemahiran atau terlibat secara langsung dengan aset ICT berkenaan.

Aktiviti perubahan atau pengubahsuaian hendaklah mematuhi spesifikasi atau kriteria yang ditetapkan dan hendaklah direkodkan serta dikawal bagi mengelakkan berlakunya ralat.

2.3.3 Sandaran (Backup)

Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang berkuat kuasa bagi memastikan sistem dapat diaktifkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah seperti yang telah digariskan dalam DKICT.

2.3.4 Kitaran Pengurusan Aset

2.3.4.1 Pindah

Pemindahan maklumat bagi menjamin keselamatan perpindahan/pertukaran maklumat dan perisian perlu dilaksanakan seperti yang telah digariskan dalam DKICT.

2.3.4.2 Pelupusan

Pelupusan media perlu mendapat kelulusan dari Pegawai Aset ICT dan mengikut prosedur pelupusan media dan selaras dengan tatacara pelupusan aset alih serta Garis Panduan Keselamatan Dokumen Elektronik dan Media Storan (jika perlu).

2.3.4.3 Kitaran Hayat

Kitaran hayat data hendaklah diuruskan mengikut Akta Arkib Negara (Akta 629). Akta Arkib Negara memberi mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun. Log sistem aplikasi disimpan untuk tempoh masa yang dipersetujui.

2.4 Manusia

Memastikan kakitangan Jabatan/Agensi Negeri, pihak ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab serta peranan masing-masing seperti yang telah digariskan dalam DKICT. Pelaksanaan ini juga perlu merangkumi:

i. Kompetensi Pengguna

ii. Kompetensi Pelaksana

3.0 KESAN

Seksyen ini menerangkan mekanisme pengesanan terhadap aktiviti yang berniat jahat, sama ada secara fizikal atau secara elektronik.

3.1 Pemantauan Berterusan

Melaksanakan pemantauan secara berterusan terhadap sistem ICT secara masa sebenar atau secara berkala menggunakan teknologi yang bersesuaian.

3.2 Anomali dan Peristiwa

3.2.1 Aliran Data Asas

Sistem yang digunakan hendaklah mengumpul data asas semasa proses pentauliahan sistem. Data asas adalah diperlukan sebagai rujukan apabila terdapat perubahan pada sistem.

3.2.2 Pengagregatan Data

Data dari pelbagai sistem hendaklah dikumpulkan.

3.2.3 Korelasi

Perhubungan/pertalian antara peristiwa dari pelbagai sistem hendaklah dilakukan bagi mengenalpasti anomali/keganjilan.

3.2.4 Pemberitahuan

CERT Negeri mengendali sebarang insiden keselamatan ICT berdasarkan Prosedur Pengendalian Insiden Keselamatan ICT.

4.0 TINDAK BALAS

Apabila berlaku insiden keselamatan ICT, Prosedur Pengendalian Insiden Keselamatan ICT akan dilaksanakan oleh CERT Negeri.

4.1 Pelantikan ICTSO

Melantik Pegawai Keselamatan ICT (ICTSO) bagi PSUKPP.

4.2 PSUKPP CERT

Menubuhkan CERT Negeri Pulau Pinang

4.3 Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT

Apabila berlaku insiden keselamatan ICT, rujuk Prosedur Pengendalian Insiden Keselamatan ICT.

4.4 Analisis

Membentangkan laporan insiden keselamatan ICT kepada Jawatankuasa Pemandu eGG.

4.4 Mitigasi

Melaksanakan Prosedur *Backup* dan *Restore* atau mengaktifkan Pelan Pemulihan Bencana (jika perlu) .

4.5 Penambahbaikan

Pelaksanaan penambahbaikan jangka panjang bagi mengelakkan insiden keselamatan ICT berulang dengan melaksanakan *Security Posture Assesment* (SPA) Secara Dalaman (setiap tahun) dan Luaran (setiap 3 Tahun).

5.0 PULIH

Melaksanakan Prosedur *Backup* dan *Restore* atau mengaktifkan Pelan Pengurusan Kesinambungan Perkhidmatan dan Pemulihan Bencana ICT (jika perlu).

5.1 Pelan Pengurusan Kesinambungan Perkhidmatan dan Pemulihan Bencana ICT

Melaksanakan Pelan Pengurusan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana ICT (ICT DRP) bagi memastikan perkhidmatan atau fungsi kritikal PSUKPP tidak terjejas walau pun berlaku gangguan.

5.2 Penambahbaikan

Melaksanakan penambahbaikan berterusan menerusi latihan simulasi Pelan Pemulihan Bencana ICT sekurang-kurangnya setahun sekali atau berdasarkan laporan tindakan penambahbaikan/pembetulan/pencegahan oleh audit dalam.

6.0 PEROLEH

Menguruskan Perolehan dan pentauliahan dilaksanakan mengikut Pekeliling Perbendaharan dan Surat Pekeliling Kewangan Negeri.

6.1 Kitar Hayat Sistem

Memastikan kitar hayat sistem mematuhi garis panduan seperti yang telah digariskan dalam DKICT.

6.6.1 Pentadbir

Fungsi pentadbir hendaklah satu peranan yang diberikan kepada pengguna tertentu dalam sistem. Peranan pentadbir boleh diberi dan dilucutkan oleh pentadbir lain. Sekurang-kurangnya dua pentadbir diperlukan dalam sistem. Semasa proses pentauliahan, pengguna pertama hendaklah diberikan peranan sebagai pentadbir. Pengguna pertama boleh melantik pengguna-pengguna lain sebagai pentadbir dengan hak yang sama. Pengguna pertama boleh dilucutkan peranan sebagai pentadbir oleh pentadbir lain.

6.6.2 Penilaian Tahap Keselamatan

Penilaian tahap keselamatan hendaklah dilaksanakan sebelum pentauliahan sistem dan secara berkala semasa pelaksanaan dan apabila terdapat perubahan pada persekitaran.

6.7 Proses Pelucutan Pentauliahan

6.7.1 Sandaran (*Backup*)

Sandaran hendaklah berjaya dilaksanakan sebelum pelucutan pentauliahan.

6.7.2 Migrasi Data

Migrasi data hendaklah berjaya dilaksanakan sebelum pelucutan pentauliah.

6.7.3 Pengurusan Perubahan

Pengurusan perubahan hendaklah dilaksanakan untuk memaklumkan kepada pihak berkaitan berhubung pelucutan pentauliahan sistem.

6.8 Pelupusan

Sila rjuk para 2.3.4.2 untuk maklumat berhubung pelupusan data.

7.0 AUDIT KESELAMATAN (ISMS)

Mempunyai pengiktirafan Pensijilan ISO/IEC 27001 :2013 ISMS oleh pihak SIRIM dan melaksanakan audit dalaman serta luaran.

7.1 Tahap Kematangan

Tahap kematangan boleh dinilai berdasarkan kepada laporan audit.

.

7.2 Audit Dalam

Melaksanakan aktiviti audit dalam berdasarkan Prosedur Audit Dalam ISMS

8.0 KUAT KUASA

Melaksanakan penguatkuasaan untuk memastikan pematuhan.

8.2 Pihak Berkuasa dan Skop Penguatkuasaan

8.2.1 CIO dan ICTSO

Pelanggaran keselamatan maklumat yang berkaitan dengan tata tertib hendaklah dikuatkuasakan oleh CIO dan ICTSO.

8.2.2 PDRM

Semua kesalahan jenayah hendaklah dikuatkuasakan oleh PDRM.

8.2.3 SKMM

SKMM merupakan agensi berkaitan untuk menguatkuasakan Akta Komunikasi dan Multimedia 1998 (Akta 588) termasuk Akta Tandatangan Digital 1997 (Akta 562).

VII. RUJUKAN

[1] "Dasar Keselamatan ICT ver. 5.3," MAMPU, Ed.: Jabatan Perdana Menteri, 2010.

[2] "Polisi Emel Rasmi Kerajaan Negeri Pulau Pinang," Pejabat Setiausaha Kerajaan Negeri Pulau Pinang, Ed.: Pusat Teknologi Maklumat dan Komunikasi Negeri, 2010.

[3] "Malaysian Public Sector ICT Security Risk Assessment Methodology," in *Surat Pekeliling Am*. vol. Bil 6: Jabatan Perdana Menteri, 2005.

[4] MAMPU, "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan," in *Pekeliling Am*. vol. Bil 1: Jabatan Perdana Menteri, 2003.

[5] "Dasar Keselamatan ICT ", B. T. Maklumat, Ed.: Kementerian Pertahanan Malaysia, 2002.

[6] "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)," in *Pekeliling Am*. vol. Bil. 1: Jabatan Perdana Menteri, 2001.

[7] "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Kerajaan," in *Pekeliling Am*. vol. Bil 3: Jabatan Perdana Menteri, 2000.

[8] *Arahan Keselamatan Malaysia*. Malaysia.

[9] BTMK, *Dasar Keselamatan ICT KKM*: Kementerian Kesihatan Malaysia, 2007.

[10] MAMPU, *Arahan Teknologi Maklumat*: Jabatan Perdana Menteri, 2007.

[11] MAMPU, "Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam," J. P. Menteri, Ed.: MAMPU, 2006, p. 29.

[12] MAMPU, "Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)," MAMPU, 2002.

[13] SIRIM, *MS ISO/IEC 27001 Information Security Management System Standard*. Malaysia, 2006.

[14] Garis Panduan Keselamatan Dokumen Elektronik Dan Media Storan.

[15] Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.