RAKKSA

RANGKA KERJA KESELAMATAN SIBER SEKTOR AWAM

KERJASAMA RAKAN STRATEGIK

MIMOS

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

MAMPU MELAKSANAKAN TRANSFORMASI

CyberSecurity MALAYSIA

APRIL 2016, VERSI 1.0

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 kementerian dan agensi Kerajaan dalam melindungi maklumat di ruang siber.

Sehubungan itu, kementerian dan agensi Sektor Awam Malaysia akan membangunkan Polisi Keselamatan Siber Jabatan masing-masing berdasarkan rangka kerja ini dan Polisi Keselamatan Siber Sektor Awam bagi mengurus dan memastikan semua aktiviti yang dilaksanakan dalam Jabatan mematuhi keperluan-keperluan yang termaktub dalam kedua-dua dokumen ini.

Di peringkat projek pula, kesemua dokumen ini perlu dirujuk dan garis panduan lebih terperinci perlu diperolehi daripada akta, peraturan dan garis panduan keselamatan siber sedia ada yang sedang berkuat kuasa bagi membangunkan Pelan Pengurusan Keselamatan Maklumat untuk projek-projek ICT.

Tahap keselamatan dan kematangan perlu ditentu berdasarkan struktur Pelan Pengurusan Keselamatan Maklumat yang disediakan oleh agensi yang melaksanakan audit keselamatan.

Rangka kerja ini dibangun berdasarkan rangka kerja sedia ada yang ditambah baik oleh pasukan projek sehingga menghasilkan satu rangka kerja keselamatan siber tempatan yang khusus bagi 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 Jabatan, 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** and (viii) **Kuat Kuasa** merentasi semua komponen bagi mengariskan skop audit dan penguatkuasaan yang dilaksanakan oleh agensi audit dan pihak berkuasa penguatkuasaan.

Rangka kerja ini juga menjelaskan tatacara pengendalian Maklumat Rahsia Rasmi dan keperluan merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) bagi urusan berkaitan pewujudan, pengkelasan, pengendalian, simpanan, premis dan pelupusan maklumat.

Aspek penting rangka kerja ini adalah untuk memastikan prinsip keselamatan yang bersesuaian dipenuhi berdasarkan penilaian risiko dan pengolahan risiko yang diperlukan.

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 itu, banyak pekeliling dan arahan berkenaan keselamatan siber telah dikeluarkan sejak tahun 2000. Walau bagaimanapun, arahan-arahan tersebut dikeluarkan secara berasingan dan mengandungi perincian yang menyukarkan perubahan untuk mengikut perkembangan teknologi. Jadi, suatu rangka kerja keselamatan siber yang menyeluruh amat diperlukan.

Rangka kerja keselamatan siber ini bertujuan memberi panduan asas serta merangkumi kesemua komponen keselamatan yang perlu diambil kira oleh kementerian dan agensi sektor awam untuk melindungi maklumat dalam ruang siber mereka.

III. SKOP

Dokumen ini menerangkan rangka kerja keselamatan siber yang mesti digunakan oleh kementerian dan agensi Sektor Awam 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)	**CNII**	Critical National Information Infrastructure / Prasarana Maklumat Kritikal Negara
d)	**CSM**	Cyber Security Malaysia
e)	**DRC**	Disaster Recovery Centre / Pusat Pemulihan Bencana
f)	**ICT**	Information Communication and Technology / Teknologi Maklumat dan Komunikasi
g)	**ICTSO**	ICT Security Officer / Pegawai Keselamatan ICT
h)	**ISMS**	Information Security Management System / Sistem Pengurusan Keselamatan Maklumat
i)	**MAMPU**	Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia
j)	**MIMOS**	MIMOS Berhad
k)	**NC4**	National Coordination and Control Centre / Pusat Kawalan dan Koordinasi Keselamatan Negara
l)	**PDRM**	Polis Diraja Malaysia
m)	**PII**	Maklumat Pengecaman Individu
n)	**SKMM**	Suruhanjaya Komunikasi Dan Multimedia Malaysia

2. Takrifan

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

b) **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

Dokumen ini hendaklah digunakan sebagai dokumen rujukan bagi agensi Sektor Awam Malaysia dalam menyediakan polisi keselamatan siber masing-masing.

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 hendaklah disemak semula secara tahunan atau lebih kerap 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 ICTadalah 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 Polisi Keselamatan Siber Jabatan yang memberi perhatian kepada isu-isu khusus Jabatan. Pelan Pengurusan Keselamatan Maklumat dengan berpandukan RAKKSSA, Polisi Keselamatan Siber Sektor Awam, Polisi Keselamatan Siber Jabatan

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 Jabatan perlu disemak dengan lebih kerap mengikut perubahan teknologi, permintaan, keperluan, undang-undang dan fungsi Jabatan.

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). Persekitaran pembolehdaya bagi RAKKSSA merangkumi jalinan kerjasama rakan strategik RAKKSSA iaitu MAMPU, CGSO, CSM dan MIMOS, tadbir urus dan pengurusan perubahan memastikan rangka kerja ini dilaksanakan dengan lancar dan diselenggara.

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 Jabatan, 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.

Jabatan hendaklah menggunakan rangka kerja ini untuk 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 Jabatan, struktur tadbir urus dan aset dalam skop perlindungan. Langkah seterusnya adalah untuk mengenal pasti kerentanan dan ancaman ke atas aset atau persekitaran fungsi dan perkhidmatan Jabatan.

Risiko merupakan kebarangkalian dan impak sesuatu insiden berlaku berpunca daripada kerentanan dan ancaman yang dikenal pasti.

Jabatan 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 Jabatan

Persekitaran perkhidmatan dan fungsi Jabatan merujuk kepada peranan Jabatan dan kebergantungannya kepada sumber lain untuk melaksanakan peranan yang ditetapkan.

1.1.1 Peranan Jabatan

Jabatan hendaklah mengenal pasti peranan dan objektifnya.

1.1.2 Kebergantungan Jabatan

Sekiranya wujud keperluan bagi Jabatan untuk berurusan dengan sumber lain dalam melaksanakan peranannya, sebarang interaksi dan kebergantungan hendaklah dikenal pasti.

1.2 Tadbir Urus

Struktur tadbir urus bagi pengurusan keselamatan siber hendaklah dikenal pasti. Struktur tadbir urus spesifik di peringkat pusat, Jabatan dan projek hendaklah diwujudkan untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat.

1.2.1 Peranan dan Tanggungjawab

Jabatan hendaklah mengenal pasti peranan dan tanggungjawab struktur tadbir urus di setiap peringkat.

1.2.2 Keperluan Perundangan dan Peraturan

Jabatan hendaklah mengenal pasti perundangan dan peraturan yang perlu dipatuhi dalam melaksanakan peranannya seperti di para 1.2.1.

1.2.3 Garis Panduan Keselamatan Siber

Jabatan hendaklah membangunkan dan mengenal pasti garis panduan keselamatan siber berkaitan berdasarkan amalan terbaik semasa dan rangka kerja ini.

1.2.4 Polisi Keselamatan Siber Jabatan

Jabatan hendaklah membangunkan polisi keselamatan siber berdasarkan Polisi Keselamatan Siber Sektor Awam dan peraturan yang sedang berkuat kuasa. Pematuhan kepada polisi keselamatan adalah mandatori.

Polisi Keselamatan Siber Jabatan hendaklah dikaji semula secara berkala dan apabila berlaku perubahan kepada Polisi Keselamatan Siber Sektor Awam dan peraturan yang sedang berkuat kuasa.

Jabatan hendaklah mengenal pasti kawasan terperingkat. **Kawasan terperingkat meliputi kawasan premis atau sebahagian daripada premis dimana rahsia rasmi disimpan atau diuruskan atau dimana kerja terperingkat dijalankan. Peranti milik persendirian dilarang penggunaannya di kawasan terperingkat.**

1.3 Aset

1.3.1 Kategori Maklumat

Mengenal pasti kategori maklumat merupakan satu langkah penting dalam memastikan perlindungan yang mencukupi dan bersesuaian dengan kategori maklumat berkenaan.

Semua maklumat yang dijana atau dikumpul oleh Jabatan hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi.

Kedua-dua kategori boleh mengandungi PII.

Maklumat Rasmi boleh juga mengandungi Data Terbuka.

1.3.1.1 Maklumat Rahsia Rasmi

Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”,

"Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

1.3.1.2 Maklumat Rasmi

Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi Kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

1.3.1.3 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.

1.3.1.4 Data Terbuka

Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan.

Jabatan hendaklah mematuhi pekeliling yang sedang berkuat kuasa.

PII dikecualikan daripada Data Terbuka.

1.3.2 Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi.

Aliran data dan komunikasi dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

Saluran komunikasi termasuk:

- Saluran komunikasi dan aliran data antara sistem dalam Jabatan.
- Saluran komunikasi dan aliran data ke sistem luar

Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

1.3.3 Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

1.3.4 Peranti Fizikal dan Sistem

Semua peranti fizikal yang digunakan dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

Peranti fizikal termasuk :

- Pelayan
- Peranti/Peralatan Rangkaian
- Komputer Peribadi
- Komputer Riba
- Telefon /peranti pintar
- Media Storan
- Peranti dengan sambungan ke internet, contohnya pengimbas, sistem kawalan akses, alat kawalan.
- Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan

1.3.5 Sistem Luaran

Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

Sistem luaran adalah sistem bukan milik Jabatan yang dihubungkan dengan sistem Jabatan. Sebagai contoh, sistem yang dikendalikan oleh organisasi awam atau swasta yang memberi/menerima maklumat daripada sistem Jabatan

1.3.6 Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

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

- Perisian Sebagai Satu Perkhidmatan
- Platform Sebagai Satu Perkhidmatan
- Infrastruktur Sebagai Satu Perkhidmatan
- Storan Pengkomputeran Awan
- Pemantauan Keselamatan

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

1.4 Risiko

Jabatan hendaklah mengenal pasti risiko yang berkaitan dengan aset yang telah dikenal pasti. Risiko adalah keberangkalian Jabatan tidak mencapai objektifnya.

Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam aset ICT Jabatan dan aset ICT luaran.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran.

Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan.

1.4.1 Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.

Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

1.4.2 Ancaman

Jabatan hendaklah mengenal pasti kedua-dua ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

1.4.3 Impak

Jabatan hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi Jabatan.

Impak teknikal melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.

Impak fungsi Jabatan melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.

1.4.4 Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko.

Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

1.4.5 Pengolahan Risiko

Pengolahan risiko merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.

Pengolahan risiko hendaklah dikenal pasti untuk menentukan sama ada perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

Baki risiko adalah risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala.

1.4.5.1 Teknologi

Teknologi hendaklah dikenal pasti untuk mengelak atau mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk menghadkan capaian logikal kepada sistem tertentu.

1.4.5.2 Proses

Jabatan hendaklah sekiranya perlu untuk pengolahan risiko, membangunkan atau mengemaskini Perekayasaan Proses, Prosedur Operasi Standard dan polisi.

1.4.5.3 Manusia

Jabatan hendaklah mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

1.4.6 Pengurusan Risiko

Jabatan hendaklah mengenal pasti struktur tadbir urus pengurusan risiko untuk:

(i) mengenal pasti kerentanan;

(ii) mengenal pasti ancaman;

(iii) menilai risiko;

(iv) menentukan pengolahan risiko;

(v) memantau keberkesanan pengolahan risiko; dan

(vi) memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

Item (v) dan (vi) di atas hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya dua kali setahun dalam mesyuarat jawatankuasa berkaitan di Jabatan.

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, Jabatan hendaklah melaksanakan prinsip keselamatan seperti berikut:

2.1.1 Prinsip "Perlu-Tahu"

Jabatan 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, Jabatan 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

Jabatan 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

Jabatan hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data Terbuka perlu dilindungi daripada segi integriti data.

2.2.1.2 Data-dalam-pergerakan

Jabatan hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

2.2.1.3 Data-dalam-penggunaan

Jabatan hendaklah menggunakan 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 oleh Jabatan.

2.2.1.4 Perlindungan Ketirisan Data

Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

2.2.2 Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, Jabatan hendaklah menggunakan teknologi dan kawalan keselamatan yang dapat melindungi data di semua peringkat saluran pemprosesan dan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam elemen persekitaran pengkomputeran yang disahkan oleh CGSO.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

- Peranti pengkomputeran peribadi
- Peranti Rangkaian
- Aplikasi
- Pelayan
- Persekitaran fizikal

2.2.2.1 Peranti Pengkomputeran Peribadi

Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem.

Contoh peranti pengkomputeran peribadi adalah komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.

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

ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada Jabatan. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

2.2.2.2 Peranti Rangkaian

Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.

Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

2.2.2.3 Aplikasi

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

Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

2.2.2.4 Pelayan

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

Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

2.2.2.5 Persekitaran Fizikal

Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

Jabatan hendaklah merujuk kepada CGSO untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.

Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

2.2.3 Kawalan Capaian

2.2.3.1 Fizikal

Jabatan hendaklah melaksanakan kawalan akses ke atas Kawasan Terperingkat. Pengesahan pengguna bagi kemasukan ke lokasi fizikal adalah berdasarkan pengenalan fizikal termasuk dokumen fizikal, pembaca biometrik, pembaca jarak dekat, 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.

Pengenalan pengguna boleh dikeluarkan kepada orang awam untuk menggunakan aplikasi e-Kerajaan dalam penyampaian perkhidmatan awam.

2.2.3.3 Pengesahan Pengguna

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

Bagi aplikasi yang mengandungi Maklumat Rahsia Rasmi atau PII, pengesahan pengguna hendaklah berdasarkan lebih daripada satu pengenalan pengguna.

Semua aplikasi Sektor Awam hendaklah menggunakan pelayan pengesahan gunasama untuk melaksanakan fungsi *Single Sign-On*.

Pengesahan pengguna adaptif merujuk kepada proses pengesahan yang memerlukan pengenalan tambahan daripada pengguna dalam keadaan tertentu. Keadaan tersebut merangkumi kelainan dalam perlakuan pengguna atau persekitaran pengkomputeran pengguna, yang menimbulkan syak bahawa kecurian pengenalan atau penipuan transaksi telah berlaku.

Fungsi pengesahan pengguna hendaklah diasingkan daripada aplikasi bagi pengurusan berpusat fungsi pengesahan. Ini bertujuan untuk memudahkan pengguna, menjimatkan kos dan membolehkan tindak balas segera terhadap ancaman.

2.2.3.4 Kebenaran Pengguna

Setelah seseorang pengguna disahkan, sistem hendaklah menentu dan memberikan akses yang dibenarkan kepada pengguna tersebut.

Kebenaran pengguna hendaklah diberi berdasarkan peranan dan tanggungjawab yang telah dikenal pasti. Aplikasi Sektor Awam disyor menggunakan kawalan capaian berdasarkan peranan.

2.2.4 Kriptografi

Kriptografi merupakan alat yang penting dan asas untuk menguruskan keselamatan ICT. Objektif utama keselamatan maklumat yang dipenuhi oleh alat kriptografi asas adalah:

(i) Kerahsiaan melalui penyulitan

(ii) Integriti data melalui fungsi hash, Kod Pengesahan Mesej (MAC) dan tandatangan digital

(iii) Jaminan pengesahan sumber data melalui MAC dan tandatangan digital

(iv) Tanpa-sangkalan melalui tandatangan digital.

(v) Jaminan pengesahan entiti melalui protokol kriptografi.

Protokol kriptografi merupakan proses langkah demi langkah antara dua atau lebih entiti untuk mencapai matlamat keselamatan. Alat kriptografi asas digunakan dalam protokol kriptografi.

Pengurusan kunci kriptografi hendaklah berdasarkan penilaian risiko.

Algoritma kriptografi yang digunakan untuk melindungi maklumat dalam pelbagai peringkat saluran pemprosesan hendaklah mematuhi peraturan semasa yang berkuat kuasa.

Penggunaan Produk Kriptografi Terpercaya adalah mandatori bagi pengendalian Maklumat Rahsia Rasmi.

Untuk mengendalikan Maklumat Rasmi, penggunaan Produk Kriptografi Terpercaya adalah digalakkan. Produk kriptografi lain yang digunapakai oleh pihak industri juga boleh digunakan untuk mengendalikan Maklumat Rasmi.

2.2.5 Pengasingan

Jabatan hendaklah memastikan pengasingan aliran data, persekitaran dan rangkaian bagi setiap kategori maklumat, iaitu Maklumat Rahsia Rasmi, Maklumat Rasmi, PII dan Data Terbuka untuk mengurangkan risiko keselamatan.

2.2.5.1 Aliran Data

Aliran data bagi Maklumat Rahsia Rasmi hendaklah diasingkan daripada aliran Data Terbuka dan PII. Selain itu, aliran data bagi empat kategori Maklumat Rahsia Rasmi hendaklah juga diasingkan.

2.2.5.2 Persekitaran

Pengasingan persekitaran untuk pembangunan, pengujian, peringkat dan produksi hendaklah dilaksanakan.

2.2.5.3 Rangkaian

Pelayan yang mengehos rangkaian hendaklah mengasingkan capaian umum dan persendirian. Pengasingan capaian persendirian mungkin perlu berdasarkan penilaian risiko. Sebagai contoh, bagi perkhidmatan untuk capaian dari internet, pelayan dan pangkalan datanya mungkin perlu dihoskan dalam segmen rangkaian yang berasingan dan membenarkan saling hubung yang terhad.

Jabatan hendaklah melaksanakan segmen rangkaian yang berasingan bagi peranti pengkomputeran peribadi milik persendirian untuk capaian internet bagi urusan tidak rasmi.

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 dilaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh personel/jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi. Hasil perubahan ini menjadi konfigurasi asas terkini.

Berdasarkan jangkaan impak perubahan, personel/jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan.

2.3.3 Sandaran

Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

Jabatan hendaklah mengambil kira spesifikasi daripada pengeluar media storan dan faktor persekitaran seperti perlindungan kebakaran dan kawalan persekitaran dalam memilih media storan dan lokasi media sandaran.

Bekas media sandaran, lokasi dan infrastruktur yang menempatkan bekas media sandaran hendaklah disahkan oleh CGSO dan sebarang perubahan hendaklah mendapat pengesahan semula daripada CGSO.

2.3.4 Kitaran Pengurusan Aset

2.3.4.1 Pindah

Pemindahan hak milik aset berlaku dalam keadaan berikut:

- Pekerja meninggalkan Jabatan disebabkan oleh persaraan, perletakan jawatan atau penugasan semula
- Aset yang dikongsi untuk kegunaan sementara
- Pemberian aset kepada Jabatan lain
- Aset dikembalikan setelah tamat tempoh pajakan

Data dalam peranti tersebut hendaklah diuruskan mengikut seksyen 2.3.4.2.

2.3.4.2 Pelupusan

Semua pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama. CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat.

Berdasarkan keputusan CGSO, pelupusan hendaklah dirujuk kepada Arkib Negara sebagai langkah kedua. Arkib Negara akan membuat keputusan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara.

Pelupusan hendaklah hanya berlaku selepas rujukan kepada kedua-dua pihak tersebut.

Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

Sanitasi data hendaklah mengikut garis panduan yang dikeluarkan oleh Kerajaan.

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.

Bagi pelupusan data, sila rujuk seksyen 2.3.4.2.

2.4 Manusia

Kakitangan Jabatan, pembekal, pakar runding dan pihak-pihak yang berkepentingan, hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan.

Asas kecekapan pengguna hendaklah dibangunkan bagi semua pekerja dalam Jabatan.

2.4.1 Kompetensi Pengguna

Kompetensi pengguna termasuk:

- Kesedaran amalan terbaik keselamatan maklumat.

  Jabatan hendaklah memupuk amalan baik Keselamatan ICT dengan mewujudkan komunikasi ICT dan program kesedaran untuk memaklumkan kepentingan keselamatan ICT.

- Kemahiran menggunakan alat keselamatan

  Jabatan hendaklah menyediakan latihan yang mencukupi kepada kakitangan berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

2.4.2 Kompetensi Pelaksana

Kakitangan yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

Pegawai keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber
- Memenuhi keperluan pembelajaran berterusan
- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber
- Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa

Pegawai Keselamatan ICT yang dilantik oleh Jabatan hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di Jabatan.

2.4.3 Peranan

Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

Kakitangan yang berperanan menguruskan aset hendaklah memastikan semua aset Jabatan dikembalikan sekiranya berlaku perubahan peranan.

Kakitangan yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti yang tersenarai dalam senarai aset dalam Nota Serah Tugas.

Kakitangan lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

3.0 KESAN

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

3.1 Pemantauan Berterusan

Terdapat banyak peralatan yang boleh digunakan untuk melakukan pemantauan berterusan terhadap sistem ICT secara masa sebenar atau secara berkala.

3.1.1 Teknologi

Teknologi yang digunakan untuk pemantauan berterusan boleh ditempatkan secara berpusat bagi menjalankan analisis terhadap log yang dikumpulkan dari pelbagai sistem.

Log sistem ICT adalah merupakan bukti yang didokumenkan dan adalah merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap akses yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log/Jejak audit hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling sedia ada yang dikeluarkan oleh Kerajaan. Log/Jejak audit hendaklah dikawal bagi mengekalkan integriti data. Analisis ke atas log/jejak audit hendaklah dilakukan secara bulanan bagi mengesan:

- Kegagalan capaian
- Penggunaan yang tidak normal, contohnya akses terhadap sistem di luar waktu kebiasaan, kekerapan akses dan tempoh penggunaan yang berlainan dari kebiasaan
- Capaian ke atas rekod-rekod terhad
- Transaksi yang tertentu
- Penggunaan sumber yang sensitif, contohnya cek kosong, pasport, sijil peperiksaan, sijil kelahiran

Pemantauan berterusan boleh dibuat secara automatik dengan menggunakan perisian tertentu sebagai contoh pengimbas virus, algoritma *check sum*, *password cracker*, semakan integriti, pengesanan penceroboh dan analisis pemantauan prestasi sistem ICT.

3.1.2 Perkongsian Wawasan Dan Kecerdasan

Pusat Kawalan dan Koordinasi Siber Negara (NC4) menyediakan platform bagi perkongsian maklumat berkaitan insiden siber untuk seluruh Prasarana Maklumat Kritikal Negara (CNII).

CNII merujuk kepada aset (fizikal dan maya), sistem dan fungsi yang penting kepada negara dan kepincangan terhadap fungsi-fungsi kritikal ini akan memberikan impak yang besar kepada pertahanan dan keselamatan negara, kekuatan ekonomi negara, imej negara, kemampuan Kerajaan untuk berfungsi, kesihatan dan keselamatan orang awam.

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

Mekanisme berjaga-jaga hendaklah disedia dan diaktifkan apabila terdapat serangan siber. NC4 menyediakan platfom bagi semua organisasi CNII untuk memberi makluman berhubung ancaman siber.

3.2.5 Kenal Pasti Impak

Agensi berkaitan hendaklah menganalis impak serangan siber untuk menentukan tindak balas yang sewajarnya.

4.0 TINDAK BALAS

Seksyen ini menerangkan tindak balas terhadap aktiviti berniat jahat yang dikesan.

Apabila berlaku insiden keselamatan siber, pelan tindak balas hendaklah dilaksanakan oleh Jabatan. Analisis lanjut, tindakan mitigasi dan penambahbaikan hendaklah dilaksanakan oleh Jabatan atas nasihat daripada agensi berkaitan.

Komunikasi kepada orang awam adalah perlu untuk menyampaikan maklumat yang tepat dan terkini.

4.1 Pelan Tindak balas

Jabatan hendahlak mematuhi peraturan semasa berhubung tindak balas keselamatan siber.

Pelan tindak balas keselamatan siber hendaklah dismulasi secara berkala dan dinilai bagi memastkan ia masih releven dan pasukan pengendali insiden adalah terlatih dan dapat mengenal pasti dan mengendalikan insiden.

Insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi hendaklah dirujuk kepada CGSO untuk tindakan selanjutnya.

4.2 Komunikasi

Komunikasi kepada orang awam bagi insiden keselamatam siber melibatkan yang Jabatan tertentu hendaklah dilakukan oleh Jabatan tersebut. Bagi kirisis nasional, komunikasi kepada orang awam hendaklah dilakukan oleh agensi berkaitan.

4.3 Analisis

Jabatan bertanggung jawab untuk melaksanakan analisis ke atas insiden keselamatan siber dan hendaklah mengemukakan laporan analisis tersebut kepada agensi berkaitan bagi tujuan rekod atau mendapatkan khidmat nasihat. Sekiranya Jabatan tidak berupaya mengendalikan insiden tersebut, analisis hendaklah dilakukan oleh agensi berkaitan.

Agensi yang mengendalikan insiden hendaklah menyediakan nasihat teknikal atau cadangan kawalan bagi menangani keretanan tersebut.

4.4 Mitigasi

Jabatan hendaklah membangunkan pelan mitigasi untuk mengurangkan kerosakan dan memastikan kesinambungan perkhidmatan.

4.5 Penambahbaikan

Jabatan hendaklah mengenal pasti dan melaksana penambahbaikan jangka panjang bagi mengelakkan insiden keselamatan siber berulang. Khidmat nasihat dari agensi pusat hendaklah diambil kira dalam membangunkan penambahbaikan jangka panjang.

5.0 PULIH

Ketersediaan maklumat adalah penting bagi penyampaian perkhidmatan Kerajaan. Sehubungan dengan itu, Pelan Pengurusan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana ICT yang efektif dan berfungsi dengan baik perlu disedia dan dilaksanakan bagi memastikan kesinambungan perkhidmatan.

5.1 Pelan Pengurusan Kesinambungan Perkhidmatan dan Pemulihan Bencana ICT

Jabatan hendaklah membangunkan Pelan Pengurusan Kesinambungan Perkhidmatan dan Pelan Pemulihan Bencana ICT (ICT DRP). Objektif pelan adalah untuk memastikan perkhidmatan atau fungsi kritikal Jabatan tidak terjejas walau pun berlaku gangguan. Pelan tersebut hendaklah menyenaraikan tugas dan tanggungjawab serta mengenal pasti keutamaan perkhidmatan kritikal yang perlu dipulihkan segera apabila berlaku gangguan/bencana.

Simulasi dan penilaian kerap ICT DRP hendaklah dilaksanakan bagi memastikan ianya kekal relevan dan untuk memastikan kesiapsiagaan pasukan pemulihan bencana.

Lokasi dan infrastruktur bagi Pusat Pemulihan Bencana (DRC) hendaklah disahkan oleh CGSO.

5.2 Penambahbaikan

Jabatan hendaklah melaksana penambahbaikan berterusan menerusi latihan simulasi terhadap plan sekurang-kurangnya setahun sekali atau apabila berlaku perubahan dalam pelan.

6.0 PEROLEH

Seksyen ini menerangkan mekanisme bagi perolehan dan pentauliahan sistem yang kukuh dan berdaya tahan daripada aktiviti berniat jahat serta merangkumi keseluruhan kitaran hayat aset.

Perolehan ini boleh dilaksanakan melalui tender, sebut harga dan rundingan terus mengikut peraturan semasa yang berkuat kuasa.

6.1 Kenal Pasti Keperluan

Jabatan hendaklah mengenal pasti keperluan sebelum sebarang perolehan dilaksanakan sama ada perolehan daripada syarikat pembekal atau pembangunan secara dalaman.

6.2 Spesifikasi Perolehan

Spesifikasi perolehan hendaklah mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan.

6.2.1 Keperluan Keselamatan

Keperluan keselamatan siber hendaklah menentukan kawalan yang diperoleh atau dibangunkan untuk memastikan pengolahan risiko bagi risiko yang dikenal pasti adalah selaras dengan rangka kerja keselamatan siber ini.

6.2.2 Pensijilan Keselamatan

Pensijilan keselamatan bagi produk dan perkhidmatan serta tahap pensijilan hendaklah ditetapkan dan terhad kepada pensijilan yang diiktiraf oleh Kerajaan.

Projek pembangunan sistem hendaklah juga tertakluk kepada keperluan pensijilan keselamatan. Pemilik sistem hendaklah memastikan pensijilan keselamatan yang berkaitan dilaksanakan ke atas sistem yang dibangunkan.

Pematuhan kepada standard keselamatan ICT adalah penting bagi memastikan keteguhan keselamatan ICT dan boleh beroperasi antara satu sama lain.

6.2.3 Kod Sumber

Semua spesifikasi perolehan dan kontrak komersial hendaklah mengandungi keperluan mandatori seperti yang berikut :

"Kerajaan hendaklah dibenarkan untuk melaksanakan semakan terhadap kod sumber"

Untuk penyataan di atas, Kerajaan adalah merujuk kepada Jabatan atau CGSO.

Bagi sistem yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori seperti yang berikut:

> "Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko."

Bagi penyataan di atas, Kerajaan adalah merujuk kepada CGSO.

6.2.4 Kitar Hayat Data

Elemen-elemen sistem yang mengandungi Maklumat Rahsia Rasmi dan Maklumat Rasmi adalah tertakluk kepada garis panduan yang sedia ada. Pemilik sistem hendaklah memastikan tindakan dilaksanakan berpandukan garis panduan ini termasuklah sanitasi data dan pelupusan media fizikal.

Semua spesifikasi perolehan dan kontrak komersial hendaklah mengandungi keperluan madatori seperti yang berikut:

> "Pembekal hendaklah memberi hak mencapai elemen sistem yang mengandungi Maklumat Rahsia Rasmi dan Maklumat Rasmi dan boleh mengambil tindakan sebagaimana yang diperlukan"

Spesifikasi perolehan hendaklah menentukan pelupusan data seperti di seksyen 2.3.4.2. Bagi Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII, pelupusan hendaklah berdasarkan garis panduan semasa.

6.2.5 Kepakaran dan Teknologi Tempatan

Perolehan produk tempatan atau yang dibangun menggunakan teknologi tempatan hendaklah diberi keutamaan dalam pembangunan dan keseluruhan kitar hayat system. Kakitangan dan sumber berkaitan sistem hendaklah dipilih untuk mengurangkan kebergantungan kepada sumber luaran, kepakaran dan teknologi asing.

6.2.6 Kompetensi Pasukan Projek

Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pensijilan minimum keselamatan maklumat bagi pasukan projek.

6.3 Pengurusan Syarikat Pembekal

Pengurusan syarikat pembekal merangkumi pengurusan pembekal yang menyediakan perkakasan dan perisian, perkhidmatan perundingan dan perkhidmatan terurus sumber luaran.

6.3.1 Pemilihan

Pemilihan syarikat pembekal hendaklah mengikut peraturan semasa yang sedang berkuat kuasa dan berdasarkan rangka kerja keselamatan siber ini. Jabatan hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan.

Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan.

Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan.

Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi.

Jawatan kuasa penilaian teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal.

Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:

(a) badan penilai pihak ketiga adalah bebas dan berintegriti;

(b) badan penilai pihak ketiga adalah kompeten;

(c) kriteria penilaian;

(d) parameter pengujian;

(e) andaian yang dibuat berkaitan dengan skop penilaian.

6.3.2 Kontrak

Kontrak hendaklah mengandungi semua elemen yang terpakai seperti yang terkandung dalam rangka kerja keselamatan siber.

6.3.3 Pemantauan

Pemantauan syarikat pembekal hendaklah dilaksanakan kepada semua perkhidmatan sumber luaran. Pemantauan syarikat pembekal hendaklah dilaksanakan selaras dengan kontrak yang dipersetujui.

6.4 Jejak Sumber

Jejak sumber merujuk kepada sejarah lengkap pergerakan aset daripada asalnya sehingga kepada Jabatan. Proses perolehan hendaklah memastikan rekod lengkap jejak sumber sepanjang kitar hayat sistem.

Jejak sumber hendaklah merangkumi keseluruhan rantaian pembekalan perkakasan dan perisian.

6.5 Kitar Hayat Sistem

Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pasang atur, penyelenggaraan dan pelupusan.

Perancangan bagi Pelan Pengurusan Keselamatan Maklumat disarankan mengikut peringkat yang diterangkan dalam kebanyakan model Kitar Hayat Sistem ICT.

6.6 Proses Pentauliahan

6.6.1 Pentadbir

Tindakan melaksanakan konfigurasi asal adalah peranan 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 dan Ujian Pemulihan

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 rujuk para 2.3.4.2 untuk maklumat berhubung pelupusan data.

7.0 AUDIT KESELAMATAN

Seksyen ini menerangkan mekanisme audit keselamatan yang diperlukan untuk mengesan amalan ketidak patuhan. Semua audit keselamatan yang dilaksanakan terhadap instalasi, persekitaran atau premis ICT Sektor Awam hendaklah mematuhi Polisi Keselamatan Siber Sektor Awam, Polisi Keselamatan Siber Jabatan, pekeliling/ peraturan/garis panduan yang berkuat kuasa.

7.1 Tahap Kematangan

Hasil audit menunjukkan tahap kematangan sesebuah jabatan yang diaudit. Setiap Jabatan mempunyai tahap kematangan yang diharapkan.

Tahap kematangan hendaklah ditentukan.

7.2 Audit Dalam

Semakan audit dalam adalah perlu bagi memastikan pematuhan terhadap peraturan dan polisi yang berkuat kuasa.

Pasukan audit dalam yang terlatih hendaklah ditubuhkan bagi melaksanakan audit dalam.

Audit Pematuhan ICT hendaklah dilaksanakan setiap tahun. Skop pematuhan ICT hendaklah meliputi pematuhan terhadap Pelan Pengurusan Keselamatan Maklumat bagi setiap projek Jabatan.

Lain-lain audit dalam termasuk audit ISMS, Pengurusan Kesinambungan Perkhidmatan dan audit Pemulihan Bencana.

7.3 Audit Luar

Semakan audit luar adalah perlu bagi memastikan pematuhan kepada peraturan dan polisi yang sedang berkuat kuasa dan hasil semakan semula audit dalam.

Audit luar hendaklah dilaksanakan oleh pihak yang tiada kepentingan terhadap Jabatan dan sistem yang diaudit.

Pensijilan khas audit luar seperti ISMS, Pengurusan Kesinambungan Perkhidmatan dan Common Criteria, hendaklah dilaksanakan oleh badan yang diiktiraf oleh Kerajaan.

8.0 KUAT KUASA

Seksyen ini menjelaskan mekanisme penguatkuasaan yang diperlukan untuk memastikan pematuhan.

8.1 Penguatkuasaan Dalaman

Pasukan penguat kuasa dalaman hendaklah diwujudkan. Hukuman bagi pelanggaran keselamatan maklumat perlu dikenalpasti dan dikuatkuasakan.

8.2 Pihak Berkuasa dan Skop Penguatkuasaan

8.2.1 Ketua Perkhidmatan

Pelanggaran keselamatan maklumat yang berkaitan dengan tata tertib hendaklah dikuatkuasakan oleh Ketua Perkhidmatan mengikut Perintah Am Bab D.

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] Arahan Keselamatan (Semakan dan Pindaan 2015).

[2] Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.

[3] Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.

[4] Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.

[5] Rancangan Malaysia ke-11.

[6] Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.

[7] Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.

[8] Dasar Kriptografi Negara 12 Julai 2013

[9] Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013.

[10] Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.

[11] Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.

[12] Arahan Ketua Pegawai Keselamatan Kerajaan 5 jun 2012 – Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam

[13] PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).

[14] Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.

[15] Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010.

[16] Akta 709 – Akta Perlindungan Data Peribadi 2010.

[17] Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam.

[18] Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 Nov 2007.

[19] Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan, 1 Jun 2007.

[20] Arahan Teknologi Maklumat, MAMPU, 2007.

[21] Akta 680 – Aktiviti Kerajaan Elektronik 2007.

[22] Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-Agensi Kerajaan

[23] Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan, 20 Oktober 2006.

[24] Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.

[25] Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006.

[26] Akta 658 – Akta Perdagangan Elektronik 2006.

[27] Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam

[28] Akta 629 – Akta Arkib Negara 2003.

[29] Akta 606 – Akta Cakera Optik 2000.

[30] Akta 588 – Akta Komunikasi dan Multimedia 1998. (in revision)

[31] Akta 562 - AktaTandatangan Digital 1997.

[32] Akta 563 – Akta Jenayah Komputer 1997.

[33] Akta 564 - Telemedicine Act 1997. (not enforced)

[34] Akta 88 – Akta Rahsia Rasmi 1972.

[35] Akta 332 – Akta Hak Cipta 1987.

[36] Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).

[37] Akta 298 – Kawasan Larangan Tempat Larangan 1959Akta 56 – Akta Keterangan 1950.

[38] National Cyber Security Policy (NCSP)

[39] Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations.

[40] Arahan Tetap Sasaran Penting.

[41] Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.

[42] Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.

[43] Perintah Am Bab D.

VIII. PENGHARGAAN

Kerjasama Rakan Strategik

Ahli Jawatankuasa Pemandu RAKKSSA

1. YBrs. Dr. Suhazimah binti Dzazali (MAMPU)
2. YBrs. Dr. Zahri bin Yunos (CSM)
3. Puan Siti Hamimah binti Rasidi (MIMOS)
4. Puan Julaila binti Engan (CGSO)

Ahli Pasukan RAKKSSA

MAMPU

1. Puan Sophia binti Hashim (Pengurus Projek)
2. Puan Nur Hidayah bt Abdullah
3. Encik Mustafa bin Abdullah
4. YBrs. Dr. Noor Hayati binti Hashim
5. Puan Norhayati binti Abdullah
6. Puan Aaishah Dato' Abu Bakar
7. Puan Norfizah binti Mat Nor
8. Encik Mohd Nawawi bin Mustafa
9. Puan Ita Nurazlin binti Mohd Sahlan

MIMOS

10. Encik Ng Kang Siong (Ketua Pasukan Pembangunan Rangka Kerja)
11. Puan Galoh Rashidah binti Haron
12. Puan Moesfa Soeheila binti Mohamad
13. Encik Alwyn Goh
14. Encik Lee Kay Win

CGSO

15. Encik Syarifuddin bin Palawa
16. Puan Surayahani bt Hasnul Bhaharin
17. Encik Hafizi bin Ibrahin
18. Encik Mohd. Syahidan bin Senin

CSM

19. Encik Mohamed Anwer Bin Mohamed Yusoff (Ketua Pasukan Kajian)
20. Puan Sabariah binti Ahmad
21. Encik Lee Hwee Hsiung
22. Encik Fazlan bin Abdullah

© RAKKSSA

PEJABAT KETUA PEGAWAI KESELAMATAN
KERAJAAN MALAYSIA