PELAN PENGURUSAN KESELAMATAN MAKLUMAT VERSI 1.0

INSTITUT TANAH DAN UKUR NEGARA (INSTUN)

PELAN PENGURUSAN KESELAMATAN MAKLUMAT VERSI 1.0

Pelan Pengurusan Keselamatan Maklumat versi 1.0 INSTUN diluluskan untuk dilaksanakan dan dikuatkuasakan mulai dari **31 Julai 2019**.

NOREHAN BINTI OMAR
PENGARAH
INSTITUT TANAH DAN UKUR NEGARA (INSTUN)

ISI KANDUNGAN

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.

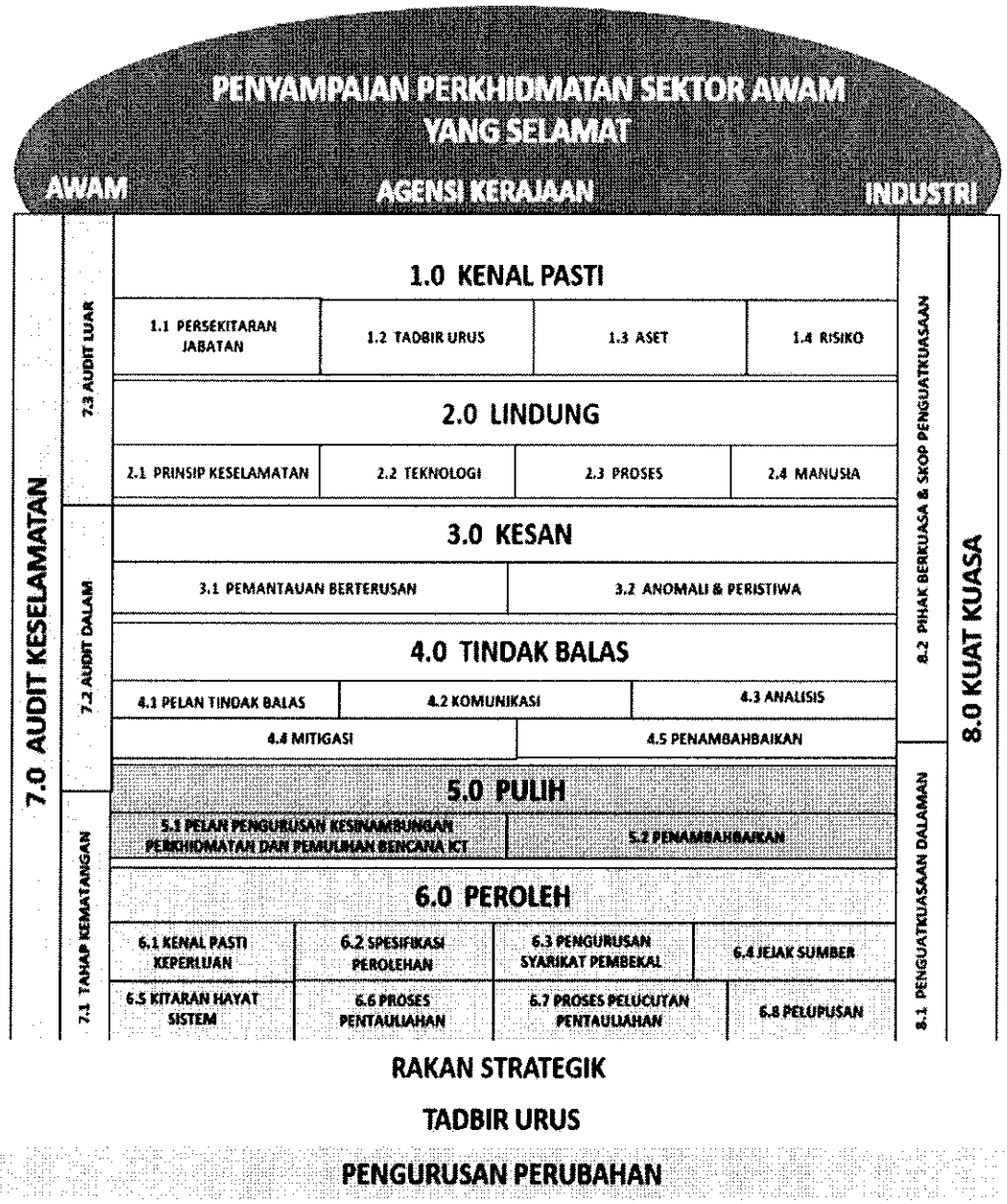
Sehubungan dengan itu, suatu rangka kerja keselamatan siber INSTUN yang menyeluruh diperlukan. Rangka kerja keselamatan siber ini bertujuan memberi panduan asas serta merangkumi kesemua komponen keselamatan yang perlu diambil kira oleh INSTUN untuk melindungi maklumat dalam ruang siber mereka.

Pelan Pengurusan Keselamatan Maklumat perlu dibangunkan di peringkat INSTUN untuk melindungi maklumat dalam ruang siber INSTUN.

SKOP

Dalam konteks dokumen ini, ruang siber ditakrifkan sebagai sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam 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.



Rajah 1 : Rangka Kerja RAKKSSA

Rangka kerja ini digunakan untuk membangunkan Pelan Pengurusan Keselamatan Maklumat (PPKM) INSTUN. Audit Keselamatan dan Kuat Kuasa merupakan dua komponen yang merentasi semua komponen.

KOMPONEN RAKKSSA

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

Rajah 2 : Komponen RAKKSSA

1. KENAL PASTI

Langkah pertama dalam perancangan keselamatan siber adalah mengenal pasti persekitaran fungsi dan perkhidmatan INSTUN, 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 INSTUN.

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

Pelan Pengurusan Keselamatan Siber adalah meliputi persekitaran perkhidmatan dan Pelan Hala Tuju INSTUN.

1.1.1. **Pelan Hala Tuju INSTUN**

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

1.1.2. **Kebergantungan INSTUN**

Kebergantungan sumber maklumat diperolehi daripada kerjasama dan ketersediaan maklumat antara INSTUN, KATS dan agensi luar.

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

1.2. Tadbir Urus

Struktur tadbir urus bagi pengurusan keselamatan siber telah dikenal pasti. Struktur tadbir urus diwujudkan untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat.

Tadbir Urus pengurusan keselamatan siber terdiri daripada:
1.2.1. **Jawatankuasa Pemandu Pengurusan Keselamatan Maklumat**
1.2.2. **Jawatankuasa Pelaksana Pengurusan Keselamatan Maklumat**

1.2.3. **Peranan dan Tanggungjawab**

1.2.3.1. **Jawatankuasa Pemandu Pengurusan Keselamatan Maklumat**

1.2.3.1.1. Menetapkan arah tuju dan strategi untuk pembangunan dan Pengurusan Keselamatan Maklumat.

1.2.3.1.2. Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga dan kewangan yang diperlukan pengurusan keselamatan maklumat berdasarkan arah tuju / strategi INSTUN dan semua agensi di bawahnya.

1.2.3.1.3. Menyelaras pembangunan program / projek ICT Kementerian dan semua agensi di bawahnya supaya mematuhi pengurusan keselamatan maklumat.

1.2.3.2. **Jawatankuasa Pelaksana Pengurusan Keselamatan Maklumat**

1.2.3.2.1. Melaksanakan tindakan pengurusan keselamatan maklumat siber.

1.2.3.2.2. Merekodkan berkaitan isu dan masalah keselamatan maklumat siber.

1.2.4. **Keperluan Perundangan dan Peraturan**

INSTUN mematuhi perundangan, peraturan, polisi dan garis panduan yang telah diwartakan oleh Kerajaan. Pelan Keselamatan Siber (PKS) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT)

INSTUN. PKS merangkumi skop perkakasan, perisian, perkhidmatan, data atau maklumat, manusia dan premis komputer dan komunikasi.

1.2.5. Garis Panduan Keselamatan Siber

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

1.2.6. Polisi Keselamatan Siber INSTUN

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

INSTUN 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 INSTUN 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 apaapa 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.
INSTUN 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 INSTUN hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

Saluran komunikasi termasuk:

1.3.2.1. Saluran komunikasi dan aliran data antara sistem dalam INSTUN.

1.3.2.2. 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 INSTUN hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

Peranti fizikal termasuk :

1.3.4.1. Pelayan
1.3.4.2. Peranti / Peralatan Rangkaian
1.3.4.3. Komputer Peribadi
1.3.4.4. Komputer Riba
1.3.4.5. Telefon / peranti pintar
1.3.4.6. Media Storan
1.3.4.7. Peranti dengan sambungan ke internet, contohnya pengimbas, sistem kawalan akses, alat kawalan.
1.3.4.8. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan

1.3.5. Sistem Luaran

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

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

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 INSTUN. 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

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

1.4. Risiko

INSTUN hendaklah mengenal pasti risiko yang berkaitan dengan aset yang telah dikenal pasti. Risiko adalah keberangkalian INSTUN tidak mencapai objektifnya.
Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam aset ICT INSTUN 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 (Vulnerability)**

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 (Threat)**

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

1.4.3. **Impak (Impact)**

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

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

Impak fungsi INSTUN 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**

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

1.4.5.3. **Manusia**

INSTUN 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**

INSTUN hendaklah mengenal pasti struktur tadbir urus pengurusan risiko untuk:
1.4.6.1. mengenal pasti kerentanan;
1.4.6.2. mengenal pasti ancaman;
1.4.6.3. menilai risiko;
1.4.6.4. menentukan pengolahan risiko;
1.4.6.5. memantau keberkesanan pengolahan risiko; dan
1.4.6.6. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

2. LINDUNG

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

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, INSTUN hendaklah melaksanakan prinsip keselamatan seperti berikut:

2.1.1. Prinsip " Perlu-Tahu"

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 dan Pengasingan Tugas

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

2.1.3. Kawalan Capaian Berdasar 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.

2.1.4. Peminimuman Data

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

2.1.5. Teknologi

Perlindungan bertujuan melindungi integriti dan kerahsiaan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh kod jahat atau program merbahaya seperti virus dan Trojan serta cubaan pencerobohan oleh anasir luar. Langkah keselamatan adalah seperti:

2.1.5.1. Memasang perisian antivirus dan Intrusion Prevention System (IPS) bagi mengesan dan menghalang kemasukannya;

2.1.5.2. Mengemas kini pattern perisian antivirus;

2.1.5.3. Konfigurasi peralatan rangkaian hendaklah mengaktifkan perkhidmatan atau nombor port yang diperlukan sahaja, mematikan penyiaran trafik (network

broadcast), menggunakan kata laluan yang selamat, dan dilaksanakan oleh pegawai yang terlatih dan dibenarkan sahaja;

2.1.5.4. Perkakasan keselamatan hendaklah dipasang bagi menghalang pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan rangkaian INSTUN; dan

2.1.5.5. Perisian penganalisis rangkaian (network analyzer) atau pengintip (sniffer) adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.

2.1.5.6. Semua trafik rangkaian daripada dalam dan ke luar INSTUN dan sebaliknya mestilah melalui firewall dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya;

2.2. Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, INSTUN 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 selamat.

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

2.2.1. Peranti Pengkomputeran Peribadi

Perkakasan ICT meliputi pelbagai peralatan ICT dan komponennya seperti komputer mikro, komputer bimbit, tablet PC, *workstation*, server, pencetak, *switch*, UPS dan sebagainya. Perkakasan yang digunakan perlu dijaga, dilindungi dan dikawal di mana:

2.2.1.1. Pengguna bertanggungjawab sepenuhnya menjaga dan melindungi segala perkakasan, komponen atau peralatan ICT di bawah kawalannya agar sentiasa berkeadaan baik dan lengkap sepanjang masa;

2.2.1.2. Setiap pengguna hendaklah memastikan semua perkakasan ICT di bawah kawalannya disimpan di tempat yang bersih dan selamat;

2.2.1.3. Pengguna dilarang memindah, menambah, membuang, atau menukar sebarang komponen atau perkakasan ICT tanpa kebenaran BPM;

2.2.1.4. Peminjaman dan pemulangan peralatan hendaklah direkodkan oleh pegawai yang telah dipertanggungjawabkan;

2.2.1.5. Setiap pengguna adalah bertanggungjawab di atas kerosakan dan kehilangan perkakasan ICT di bawah kawalannya;

2.2.1.6. Setiap pengguna hendaklah melaporkan sebarang bentuk penyelewengan atau salah guna perkakasan ICT kepada ICTSO;

2.2.1.7. Penyelenggaraan peralatan ICT hanya boleh dilakukan oleh pegawai atau pihak yang dibenarkan sahaja; dan

2.2.1.8. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap dan mengikut prosedur pelupusan aset yang dikuatkuasakan. Maklumat atau kandungan dokumen hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilakukan. Sekiranya maklumat perlu disimpan, penduaan bolehlah dilakukan.

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.

Infrastruktur rangkaian mesti dikawal dan diurus dengan baik bagi melindungi aset ICT dan aplikasi ICT di dalam rangkaian. Langkah-langkah keselamatan rangkaian adalah seperti berikut:

2.2.2.1. Hanya warga INSTUN sahaja yang dibenarkan menggunakan rangkaian INSTUN. Pengguna luar yang hendak menggunakan kemudahan rangkaian INSTUN hendaklah dengan kebenaran BPM;

2.2.2.2. Tanggungjawab atau kerja-kerja operasi rangkaian INSTUN adalah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

2.2.2.3. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh, selamat dan bebas dari risiko seperti banjir, kilat, gegaran, habuk dan sebagainya;

2.2.2.4. Peralatan rangkaian hendaklah dikawal dan hanya boleh dicapai oleh pegawai yang dibenarkan sahaja;

2.2.2.5. Konfigurasi peralatan rangkaian hendaklah mengaktifkan perkhidmatan atau nombor port yang diperlukan sahaja, mematikan penyiaran trafik (network broadcast), menggunakan kata laluan yang selamat, dan dilaksanakan oleh pegawai yang terlatih dan dibenarkan sahaja;

2.2.2.6. Semua trafik rangkaian daripada dalam dan ke luar INSTUN dan sebaliknya mestilah melalui firewall dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya;

2.2.2.7. Semua permohonan baru untuk mendapat sambungan rangkaian mestilah melalui pentadbir rangkaian;

2.2.2.8. Pengguna adalah dilarang untuk menukar atau meletakkan alamat IP di dalam komputer masingmasing tanpa kebenaran;

2.2.2.9. Sebarang permohonan untuk menggunakan statik IP hendaklah melalui pentadbir rangkaian;

2.2.2.10. Kemudahan dial-up hanya dibenarkan untuk tujuan rasmi dan permohonan dibuat melalui pentadbir rangkaian. Pengguna yang menggunakan kemudahan dial-up hendaklah mengimbas keseluruhan komputer dahulu sebelum membuat penyambungan semula ke rangkaian INSTUN;

2.2.2.11. Perkakasan keselamatan hendaklah dipasang bagi menghalang pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan rangkaian INSTUN; dan

2.2.2.12. Perisian penganalisis rangkaian (network analyzer) atau pengintip (sniffer) adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.

Ciri-ciri keselamatan dan keperluan pengurusan bagi semua servis rangkaian perlu dikenalpasti dan dinyatakan dalam perjanjian yang melibatkan servis rangkaian.

2.2.3. **Aplikasi**

Perisian aplikasi digunakan oleh manusia 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.

2.2.4. **Pelayan**

Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat. Untuk memastikan server sentiasa selamat dari pencerobohan atau gangguan beberapa langkah boleh diambil seperti:

2.2.4.1. Semua server hendaklah diletakkan di pusat data atau bilik khas yang mempunyai sistem keselamatan yang baik. Pintu bilik hendaklah sentiasa tertutup dan berkunci;

2.2.4.2. Sistem penghawa dingin hendaklah dihidupkan 24 jam sehari. Suhu persekitaran hendaklah berada di dalam lingkungan 20 – 25 darjah Celsius dan kelembapan di paras 50.7%;

2.2.4.3. Kesemua peralatan komputer di bilik server hendaklah dilengkapi dengan kemudahan UPS atau Generator;

2.2.4.4. Alat pemadam api hendaklah diletakkan di tempat yang mudah dilihat, tidak terhalang oleh sesuatu, mudah dicapai, tidak melepasi tarikh luput serta diselenggarakan dengan baik;

2.2.4.5. Hanya pegawai atau pegawai yang dibenarkan sahaja yang boleh memasuki pusat data;

2.2.4.6. Kontraktor/vendor dibenarkan memasuki pusat data dengan diiringi oleh seorang pegawai/pegawai BPM dan hendaklah mendaftar di buku log yang disediakan; dan

2.2.4.7. Setiap server hendaklah dilabelkan bagi memudahkan pentadbir sistem menjalankan tugas.

2.2.5. **Persekitaran Fizikal**

Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT. Bertujuan untuk mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat. Langkah keselamatan yang perlu diikuti adalah seperti: Mengenal pasti kawasan keselamatan fizikal. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset;

2.2.5.1. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

2.2.5.2. Menyediakan tempat atau bilik khas untuk pelawatpelawat;

2.2.5.3. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan pegawai yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

2.2.5.4. Mengadakan kaunter kawalan;

2.2.5.5. Memasang alat penggera, kamera litar tertutup (CCTV) dan seumpamanya;

2.2.5.6. Mewujudkan perkhidmatan kawalan keselamatan;

2.2.5.7. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;

2.2.5.8. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;

2.2.5.9. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan

2.2.5.10. Mereka bentuk dan melaksanakan perlindungan fizikal dan panduan untuk pegawai yang bertugas di kawasan terhad.

2.2.6. **Kawalan Capaian**

2.2.6.1. **Fizikal**

INSTUN 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.

2.2.6.2. **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.

2.2.6.3. **Pengesahan Pengguna**

Pengesahan pengguna kepada aplikasi INSTUN 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 INSTUN 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.

2.2.6.4. **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. Ia merupakan kemudahan yang tertakluk kepada peraturan INSTUN 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
e. Pentadbir sistem/e-mel boleh membeku atau menamatkan akaun pengguna yang telah tamat perkhidmatan, bertukar atau bercuti/berkursus panjang selepas 1 hari bekerja.

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

2.2.6.5. **Kriptografi**

Kriptografi merupakan alat yang penting dan asas untuk menguruskan keselamatan ICT.

Objektif utama keselamatan maklumat yang dipenuhi oleh alat kriptografi asas adalah:
- Kerahsiaan melalui penyulitan.
- Integriti data melalui fungsi hash, Kod Pengesahan Mesej (MAC) dan tandatangan digital.
- Jaminan pengesahan sumber data melalui MAC dan tandatangan digital.
- Tanpa-sangkalan melalui tandatangan digital.
- Jaminan pengesahan entiti melalui protokol kriptografi.

Pengguna hendaklah membuat *encryption* ke atas maklumat sensitif atau terperingkat. Penggunaan teknologi *encryption* bergantung kepada kelulusan ICTSO dan CIO serta tertakluk kepada kesediaan peruntukan. Langkah-langkah berikut perlu dipatuhi:

- Pengguna yang terlibat dalam menguruskan transaksi maklumat penting secara elektronik hendaklah menggunakan tandatangan digital yang dikeluarkan oleh Pihak Berkuasa Persijilan (*Certification Authority*) yang ditauliahkan oleh Kerajaan Malaysia.
- Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

2.2.6.6. **Pengasingan**

INSTUN 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.

Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan kepada tahap sensitiviti masing-masing.

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada kerajaan. Setiap maklumat yang dikelaskan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad mestilah diuruskan mengikut peringkat keselamatan seperti dinyatakan dalam dokumen Arahan Keselamatan.

2.2.7. **Aliran Data**

Penghantaran dokumen yang telah diklasifikasikan mesti mengikut Arahan Keselamatan, di bab Keselamatan Dokumen:
Seksyen V: Penghantaran Dokumen Terperingkat

Seksyen VI: Membawa Dokumen Terperingkat Keluar Pejabat
Seksyen VII: Pelepasan Perkara Terperingkat

2.2.8. **Persekitaran**

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

2.2.9. **Rangkaian**

Pelayan yang mengehos rangkaian hendaklah mengasingkan capaian umum dan persendirian. Pengasingan capaian persendirian mungkin perlu berdasarkan penilaian risiko.

Perkhidmatan untuk capaian dari internet, pelayan dan pangkalan data INSTUN perlu dihoskan dalam segmen rangkaian yang berasingan dan membenarkan saling hubung yang terhad.

Segmen rangkaian yang berasingan dikonfigurasi bagi peranti pengkomputeran peribadi milik persendirian untuk capaian internet bagi urusan tidak rasmi.

2.2.10. **Proses**

2.2.10.1. **Konfigurasi Asas**

Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

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

2.2.10.2. **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.

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.

2.2.10.3. **Sandaran (Backup)**

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. Penduaan dari server atau komputer ke media storan lain perlu dilakukan dari masa ke semasa untuk mengelak kehilangan data sekiranya berlaku kerosakan hard disk.

Kekerapan penduaan data bergantung kepada keperluan operasi dan kepentingan data tersebut samada perlu kepada harian, mingguan atau pun bulanan.

Penduaan sistem aplikasi dan sistem pengoperasian perlu diadakan sekurang-kurangnya sekali bagi setiap versi. Penduaan yang melibatkan saiz data yang besar hendaklah dibuat di sebelah malam untuk mengelakkan kesesakan rangkaian serta mengganggu prestasi server.

Penduaan data yang penting dan kritikal dicadangkan dibuat dua (2) salinan dan setiap satu disimpan di lokasi offsite yang berasingan bagi mengelakkan kemusnahan atau kerosakan fizikal disebabkan oleh bencana seperti kebakaran, banjir atau sebagainya.

Sistem penduaan sedia ada hendaklah diuji sekurang-kurangnya setahun sekali bagi memastikan ianya dapat berfungsi, boleh dipercayai dan berkesan apabila digunakan (restoration) khususnya pada waktu kecemasan.

Faktor ketahanan dan jangka hayat media storan perlu di ambil kira dalam melakukan penduaan serta merancang penyalinan semula kepada media storan yang baru.

2.2.11. **Kitaran Pengurusan Aset**

2.2.11.1. **Pindah**

Pemindahan hak milik aset berlaku dalam keadaan berikut:

- Pekerja meninggalkan INSTUN 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 2.2.7.

2.2.11.2. **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.

2.2.11.3. **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.

2.3. Manusia

Kakitangan INSTUN, 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 INSTUN.

2.3.1. Kompetensi Pengguna

Kompetensi pengguna termasuk:

2.3.1.1. Kesedaran amalan terbaik keselamatan maklumat.

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

2.3.1.2. Kemahiran menggunakan alat keselamatan

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

2.3.2. Kompetensi Pelaksana

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

Pegawai keselamatan ICT hendaklah :

2.3.2.1. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber yang berkaitan

2.3.2.2. Memenuhi keperluan pembelajaran berterusan

2.3.2.3. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber

2.3.2.4. Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa

Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di INSTUN.

2.3.3. **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 INSTUN dikembalikan sekiranya berlaku perubahan peranan.

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

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

3. KESAN

INSTUN mengesan ancaman serangan aktiviti yang berniat jahat secara dua kaedah iaitu fizikal atau elektronik

Antara aktiviti yang dilaksanakan adalah :

3.1. Pemantauan Berterusan melalui Teknologi dan Perkongsian Wawasan dan Kecerdasan

3.1.1. Dilaksanakan secara masa sebenar dan secara berkala

3.1.2. Pemantauan berterusan terhadap log-log dari pelbagai sumber untuk analisis dan disimpan mengikut arahan / pekeliling sedia ada yang dikeluarkan oleh Kerajaan.

3.1.3. Pemantauan berterusan secara automatik menggunakan perisian tertentu seperti antivirus, laporan pemantauan dari MAMPU / KATS / GITN, pemantauan prestasi sistem ICT dan sebagainya

3.1.4. Pemantauan berkala menggunakan perkakasan dan perisian rangkaian dan melaksanakan aktiviti berkaitan Keselamatan seperti Security Posture Assessment (SPA)

3.1.5. Laporan bulanan dan laporan aktiviti berkaitan

3.2. Anomali dan Peristiwa

3.2.1. Penggunaan Aliran Data Asas sebagai rujukan

3.2.2. Pengagregatan Data bagi pemusatan data

3.2.3. Korelasi antara peristiwa dari pelbagai sistem bagi pengenalpastian anomali / keganjilan

3.2.4. Pemberitahuan / Pemakluman perhubungan bersama MAMPU / NACSA sekiranya berlaku ancaman siber

3.2.5. Mengenalpasti impak serangan siber dan menentukan tindak balas yang sewajarnya

4. TINDAK BALAS

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

Komunikasi kepada orang awam adalah perlu untuk menyampaikan maklumat yang tepat dan terkini (jika ada keperluan).

4.1. Pelan Tindak Balas

INSTUN wajib mematuhi peraturan semasa berhubung tindak balas keselamatan siber. Pelan tindak balas keselamatan siber hendaklah disimulasi secara berkala dan dinilai bagi memastkan ia masih releven dan pasukan pengendali insiden adalah terlatih dan dapat mengenal pasti untuk mengendalikan insiden.

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

Pelan tindak balas diwujudkan selaras prosedur dan tatacara keperluan Polisi Keselamatan Siber INSTUN.

4.2. Pelantikan ICTSO INSTUN

Pegawai Keselamatan ICT (ICTSO) adalah dilantik dari kalangan pengurusan tertinggi di Bahagian Teknologi Maklumat (BTM) INSTUN.

Peranan dan tanggungjawab (ICTSO) adalah seperti berikut:

4.2.1. Mengurus keseluruhan program-program keselamatan ICT INSTUN;
4.2.2. Memberi penerangan kepada pengguna berkenaan Polisi Keselamatan Siber INSTUN;
4.2.3. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber INSTUN;
4.2.4. Bertindak sebagai pengurus Computer Emergency Response Team ICT (INSTUN CERT);
4.2.5. Mengurus tindakan audit, mengkaji semula, merumus tindak balas berdasarkan hasil penemuan dan menyediakan laporan;
4.2.6. Memberi amaran terhadap kemungkinan berlakunya ancaman keselamatan ICT dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang sesuai;
4.2.7. Memaklumkan insiden keselamatan ICT kepada CIO dan melaporkannya kepada Computer Emergency Response Team ICT (INSTUN CERT);
4.2.8. Bekerjasama dengan pihak-pihak yang berkaitan dalam mengenal pasti punca insiden dan memperakukan langkahlangkah baik pulih dengan segera; dan
4.2.9. Menyedia dan melaksana program-program kesedaran mengenai keselamatan ICT.

4.3. INSTUN CERT

Pengendalian Insiden Keselamatan ICT di INSTUN adalah berpandukan Surat Pekeliling Am Bil. 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam yang dikeluarkan oleh MAMPU bertarikh 9 November 2006.

Pasukan pengendali insiden di peringkat INSTUN iaitu *Computer Emergency Response Team* (INSTUN CERT) telah ditubuhkan bagi memperkemaskan pengurusan pengendalian insiden keselamatan ICT serta bertindak sebagai *first level support* kepada NACSA, MKN dalam mengendali insiden, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada pegawai di bawah kawalannya.

Tugas INSTUN CERT INSTUN secara amnya adalah seperti berikut:

4.3.1. Menerima dan mengambil tindakan ke atas insiden keselamatan yang dilaporkan;

4.3.2. Memberi amaran terhadap kemungkinan berlakunya ancaman keselamatan ICT dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang sesuai di peringkat INSTUN;

4.3.3. Menyebarkan maklumat bagi membantu pengukuhan keselamatan ICT di agensi dari semasa ke semasa;

4.3.4. Menyediakan khidmat nasihat kepada kepada pegawai dalam mengesan, mengenalpasti dan menangani sesuatu insiden keselamatan;

4.3.5. Bekerjasama dengan pihak-pihak yang berkaitan seperti KATS, Malaysian Computer Emergency Response Team (MyCERT), National Cyber Security Agency (NACSA), pembekal, Internet Service Provider (ISP) dan agensi-agensi penguatkuasa; dan

4.3.6. Menyedia dan melaksana program-program kesedaran mengenai keselamatan ICT.

4.4. Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT INSTUN CERT

Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT INSTUN CERT mengandungi proses dalam pengendalian insiden keselamatan ICT iaitu :

4.4.1. Pentadbiran Incident Response Handling (IRH);
4.4.2. Pengurusan Pengendalian Insiden;
4.4.3. Penyebaran Maklumat;
4.4.4. Penyelarasan Pengurusan Insiden;
4.4.5. Panduan Komunikasi Pengendalian Insiden Secara Jarak Jauh;
4.4.6. Template Borang IRH 1.0 : Maklumat Pengendalian Insiden Keselamatan ICT;
4.4.7. Template Borang IRH 1.1 : Maklumbalas Tindakan Susulan Dari Pengendalian Insiden Keselamatan ICT;
4.4.8. Template Laporan Analisis Fail Log;
4.4.9. Template Laporan Imbasan Hos; dan
4.4.10. Template Laporan Kronologi Insiden Keselamatan ICT.

4.5. Komunikasi

Komunikasi kepada orang awam bagi insiden keselamatan siber yang melibatkan INSTUN tertentu hendaklah dilakukan oleh INSTUN (jika ada keperluan).

4.6. Analisis

INSTUN 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 (jika ada keperluan). Sekiranya INSTUN tidak berupaya mengendalikan insiden tersebut, analisis hendaklah dilakukan oleh KATS / MAMPU / NACSA.

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

4.7. Mitigasi

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

4.8. Penambahbaikan

INSTUN hendaklah mengenal pasti dan melaksana penambahbaikan jangka panjang bagi mengelakkan insiden keselamatan siber berulang. Khidmat nasihat dari agensi pusat (KATS / MAMPU / NASCA) hendaklah diambil kira dalam membangunkan penambahbaikan jangka panjang.

5. 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 ICT

Pelan Pemulihan Bencana (DRP) INSTUN adalah proses, polisi dan prosedur yang berkaitan dengan persiapan pemulihan atau kesinambungan infrastruktur kritikal di INSTUN akibat bencana alam atau gangguan disebabkan perbuatan manusia. DRP adalah sebahagian dari Pelan Pengurusan Kesinambungan Perkhidmatan. Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) INSTUN melibatkan perancangan untuk memastikan semua perkhidmatan kritikal dapat berfungsi di tengah-tengah peristiwa yang mengganggu, sementara DRP INSTUN lebih fokus kepada IT atau teknologi maklumat yang menyokong fungsi utama atau perkhidmatan kritikal di INSTUN sebelum, semasa dan selepas gangguan/bencana.

5.2. Penambahbaikan

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

6. PEROLEHAN

Perkara Perolehan ini menerangkan kaedah bagi perolehan sama ada peralatan ICT atau pun aplikasi serta pentauliahan peralatan dan aplikasi supaya ianya kukuh dan berdaya tahan daripada aktiviti pencerobohan.

Perolehan ini dibuat mengikut perkara-perkara berikut :

- Kenalpasti Keperluan
- Spesifikasi Perolehan
- Pengurusan Syarikat Pembekal
- Jejak Sumber
- Kitar Hayat Sistem
- Proses Pentauliahan
- Proses Pelucutan Pentauliahan
- Pelupusan

6.1. Kenalpasti Keperluan

Bahagian Teknologi Maklumat perlu mengenalpasti keperluan untuk perolehan peralatan ICT atau pun aplikasi sebelum sebarang perolehan dibuat. Bahagian juga perlu untuk mengenalpasti sama ada perolehan yang hendak dilaksanakan itu daripada syarikat pembekal atau pun pembangunan secara dalaman.

6.2. Spesifikasi Perolehan

Spesifikasi perolehan hendaklah mengandungi perkara-perkara tertentu yang ditetapkan seperti:

- keperluan keselamatan
- pensijilan keselamatan produk
- ketersediaan kod sumber
- keperluan pelupusan data
- keutamaan terhadap teknologi dan kepakaran tempatan, 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. Setiap projek pembangunan aplikasi perlu mengikut garis panduan pensijilan keselamatan yang telah ditetapka. Pematuhan kepada standard keselamatan ICT adalah penting untuk memastikan keteguhan serta keselamatan ICT supaya ianya tidak mudah diceroboh serta berdaya tahan. Ianya juga perlu dipastikan boleh beroperasi antara satu sama lain. Syarikat pembekal juga perlu mematuhi Polisi Keselamatan Siber INSTUN yang telah disediakan.

6.2.3. Kod Sumber

Keperluan mandatori yang disarankan oleh Pejabat Ketua Pegawai Keselamatan Malaysia (CGSO) bagi semua spesifikasi perolehan dan kontrak komersial iaitu Kerajaan hendaklah dibenarkan untuk melaksanakan semakan terhadap kod sumber, perlu dimasukkan dan diikuti ketika pembangunan aplikasi.

Manakala bagi aplikasi yang mengendalikan Maklumat Rahsia Rasmi, keperluan mandatori seperti Pembekal hendaklah membenarkan pihak Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko, juga hendaklah dimasukkan.

6.2.4. **Kitar Hayat Data**

Ciri-ciri aplikasi yang mengandungi Maklumat Rahsia Rasmi dan Maklumat Rasmi adalah tertakluk kepada garis panduan yang sedia ada. Pemilik aplikasi tersebut perlu memastikan tindakan yang hendak dilaksanakan berpandukan garis panduan yang ditetapkan itu. Ianya juga termasuk sanitasi data dan pelupusan media fizikal.

Dalam kitar hayat data, semua spesifikasi perolehan dan kontrak komersial perlu mengambilkira keperluan madatori yang telah ditetapkan iaitu pembekal hendaklah memberi hak mencapai elemen sistem yang mengandungi Maklumat Rahsia Rasmi dan Maklumat Rasmi dan boleh mengambil tindakan sebagaimana yang diperlukan.

Sebarang media storan yang mengandungi data yang hendak dilupuskan, khidmat nasihat dan rujukan kepada Pegawai Keselamatan ICT INSTUN perlu dibuat sebagai langkah pertama sebelum pelupusan dilaksanakan.

Langkah kedua iaitu merujuk kepada CGSO dan Jabatan Arkib Negara (jika ada keperluan) dan perlu mengikut garis panduan yang dikeluarkan oleh Kerajaan.

6.2.5. **Kepakaran dan Teknologi Tempatan**

Keutamaan perlu diberikan kepada teknologi dan kepakaran tempatan dalam proses pembangunan dan keseluruhan kitar hayat system. Kepakaran, pembangun aplikasi dan juga sumber dalam pembangunan aplikasi hendaklah di pilih secara teliti bagi mengurangkan kebergantungan terhadap sumber, kepakaran dan teknologi luaran.

6.2.6. **Kompetensi Pasukan Projek**

Pensijilan Keselamatan perlu dimasukkan dalam dokumen penyediaan spesifikasi perolehan sebagai satu syarat kepada pasukan projek bagi memastikan pasukan projek tersebut mematuhi keselamatan pembangunan aplikasi. Selain daripada itu juga, pengalaman pasukan projek berdasarkan perolehan yang dibuat juga perlu dinyatakan dalam dokumen penyediaan spesifikasi perolehan. Pasukan projek juga memerlukan pensijilan yang diiktiraf dalam bidang yang telah dipilih untuk menawarkan perkhidmatan.

6.3. Pengurusan Syarikat Pembekal

Pengurusan syarikat pembekal merangkumi pengurusan pembekal yang menyediakan perkakasan dan perisian, perkhidmatan perundingan dan perkhidmatan terurus sumber luaran. Syarikat pembekal juga perlu mempunyai jawatankuasa tadbirurus bagi menguruskan projek perolehan yang dimenangi supaya ianya berjalan dengan lancar dan berkesan.

6.3.1. **Pemilihan**

Pemilihan syarikat pembekal hendaklah mengikut peraturan semasa yang sedang berkuat kuasa dan berdasarkan rangka kerja keselamatan siber. INSTUN 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:

6.3.1.1. badan penilai pihak ketiga adalah bebas dan berintegriti;
6.3.1.2. badan penilai pihak ketiga adalah kompeten;
6.3.1.3. kriteria penilaian;
6.3.1.4. parameter pengujian;
6.3.1.5. andaian yang dibuat berkaitan dengan skop penilaian.

6.4. Kontrak

Kontrak hendaklah mengandungi semua elemen yang terpakai seperti yang terkandung dalam rangka kerja keselamatan siber. Kontrak yang ditandatangani juga perlu mengandungi SLA dan perlu dipatuhi oleh syarikat pembekal yang dilantik. Tempoh kontrak serta terma yang telah ditetapkan dalam kontrak tersebut hendaklah di semak dan disahkan oleh Penasihat Undang-Undang.

6.5. Pemantauan

Pemantauan syarikat pembekal hendaklah dilaksanakan kepada semua perkhidmatan sumber luaran yang mana ianya hendaklah dilaksanakan selaras dengan kontrak yang telah dipersetujui. Mesyuarat kemajuan juga perlu diadakan bagi memantau pelaksanaan projek perolehan tersebut mengikut masa yang ditetapkan sebagaimana yang dipersetujui dalam kontrak. Syarikat pembekal juga perlu mematuhi Polisi Keselamatan Siber INSTUN. Pembekal juga juga perlu mengisi borang Akta Rahsia Rasmi Kerajaan bagi tujuan keselamatan sekiranya sesuatu perkara telah dilakukan oleh pihak syarikat.

6.6. Jejak Sumber

Jejak sumber merujuk kepada sejarah lengkap pergerakan aset daripada perolehan (asal). Proses perolehan hendaklah memastikan rekod lengkap jejak sumber sepanjang kitar hayat sistem. Ianya juga hendaklah keseluruhan rantaian pembekalan perkakasan dan perisian.

6.7. 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.

6.8. Proses Pentauliahan

6.8.1. 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.

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.

6.8.2. **Penilaian Tahap Keselamatan**

Penilaian tahap keselamatan hendaklah dilaksanakan sebelum pentauliahan sistem dan secara berkala semasa pelaksanaan dan apabila terdapat perubahan pada persekitaran. Pengujian keberkesanan capaian aplikasi juga perlu dibuat supaya daya tahan capaian aplikasi tersebut dapat diukur dan ditambahbaik. Selain daripada itu, pengujian pencerobohan terhadap aplikasi juga perlu dilaksanakan supaya ianya selamat daripada sebarang cubaan pencerobohan terhadap aplikasi tersebut.

6.8.3. **Proses Pelucutan Pentauliahan**

6.8.3.1. **Sandaran dan Ujian Pemulihan**

Sandaran hendaklah berjaya dilaksana sebelum pelucutan pentauliahan.

6.8.3.2. **Migrasi Data**

Migrasi data hendaklah berjaya dilaksanakan sebelum pelucutan pentauliah.

6.8.3.3. **Pengurusan Perubahan**

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

6.9. Pelupusan

Sebarang media storan yang mengandungi data yang hendak dilupuskan, khidmat nasihat dan rujukan perlu dirujuk kepada Pegawai Keselamatan ICT INSTUN.

Pelupusan aset ICT perlu mengikut garis panduan yang telah ditetapkan melalui Pekeliling Perbendaharaan Malaysia AM 2.6. mengikut garis panduan yang dikeluarkan oleh Kerajaan.

7. AUDIT KESELAMATAN

INSTUN telah berjaya mendapat pengiktirafan Pensijilan ISO/IEC 27001:2013 oleh pihak SIRIM pada 2014. Skop pensijilan adalah Sistem Pengurusan Keselamatan Maklumat di Pusat Data dan Sistem Pengurusan Kursus INSTUN (eSPEK).

Polisi dan prosedur yang terlibat termasuklah Pelan Keselamatan Siber, Data Recovery Plan (DRP) dan Standard Operating Procedure (SOP).

Audit Pensijilan telah dimulakan pada tahun 2014. Pemantauan Pematuhan Audit juga dilaksanakan setiap tahun.

7.1. Audit Dalam

Semakan audit dalam dilaksanakan pada setiap tahun bagi memastikan pematuhan terhadap peraturan dan polisi yang berkuat kuasa. INSTUN menggunakan khidmat juruaudit dari Bahagian Teknologi Maklumat atau dari agensi di bawah KATS.

7.2. Audit Luar

Semakan Audit Luar dilaksanakan oleh Juruaudit yang bertauliah daripada SIRIM.

8. KUAT KUASA

Seksyen ini menjelaskan mekanisme penguatkuasaan yang diperlukan untuk memastikan pematuhan.

8.1. Penguatkuasaan Dalaman

Jenayah di alam siber memerlukan pegawai-pegawai penyiasat yang berkemahiran tinggi dan kerjasama strategik antara agensi-agensi penguatkuasaan di dalam dan luar negara. Jika jenayah di alam nyata meninggalkan kesan DNA, penjenayah siber pula meninggalkan jejak bukti digital. Pemasangan Content Filtering telah dilaksana di INSTUN untuk memastikan tahap keselamatan yang selamat untuk capaian internet.

Pelanggaran dasar keselamatan maklumat ICT secara sengaja akan menyebabkan:
8.1.1. Kehilangan hak capaian ke atas sumber maklumat;
8.1.2. Membekukan atau menamatkan akaun emel pegawai
8.1.3. Penilaian prestasi kerja yang buruk;
8.1.4. Dikenakan tindakan tatatertib;
8.1.5. Digantung kerja atau ditamatkan perkhidmatan;
8.1.6. Ditamatkan kontrak;
8.1.7. Dikenakan tindakan undang-undang.

8.2. Pihak Berkuasa dan Skop Penguatkuasaan

8.2.1. Ketua Perkhidmatan

Sekiranya perkara ini berlaku, tindakan tatatertib di bawah Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 [P.U(A)395/1993] akan diambil setelah dibuktikan

kesalahannya. Pegawai yang didapati membocorkan maklumat/dokumen terperingkat Kerajaan adalah disifatkan telah melanggar peraturan 4, P.U(A)395/1993.

Pelanggaran ini boleh menyebabkan pegawai awam dikenakan tindakan tatatertib sehingga hukuman buang kerja. Pegawai juga boleh dikenakan tindakan undang-undang di bawah mana-mana undang-undang yang berkaitan.

8.2.2. Polis DiRaja Malaysia (PDRM)

Semua kesalahan jenayah hendaklah dikuatkuasakan oleh PDRM. Sekiranya berlaku sebarang insiden jenayah terhadap dokumen terperingkat, pihak INSTUN akan melaporkan kepada balai polis yang berhampiran.

8.2.3. Suruhanjaya Komunikasi dan Multimedia (SKMM)

Keperluan perundangan atau peraturan-peraturan lain yang berkaitan perlu dipatuhi oleh semua pengguna ICT INSTUN dari semasa ke semasa. SKMM merupakan agensi berkaitan untuk menguatkuasakan Akta Komunikasi dan Multimedia 1998 (Akta 588) termasuk Akta Tandatangan Digital 1997 (Akta 562).

PENUTUP

Pelan Pengurusan Keselamatan Maklumat merupakan satu dokumen *blue print* bagi pelaksanaan keselamatan maklumat siber yang perpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA). Pelan ini memfoukuskan 8 komponen utama di dalam RAKKSSA. Pelan ini diharap dapat mengoptimumkan keselamatan maklumat di INSTUN.

RUJUKAN

1. Dasar Keselamatan ICT INSTUN
2. Arahan Keselamatan (Semakan dan Pindaan 2015).
3. Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.
4. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
5. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.
6. Rancangan Malaysia ke-11.
7. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.
8. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
9. Dasar Kriptografi Negara 12 Julai 2013
10. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013.
11. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.
12. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
13. Arahan Ketua Pegawai Keselamatan Kerajaan 5 jun 2012 – Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam
14. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).
15. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.
16. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010.
17. Akta 709 – Akta Perlindungan Data Peribadi 2010.
18. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam.
19. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 Nov 2007.
20. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan, 1 Jun 2007.
21. Arahan Teknologi Maklumat, MAMPU, 2007.
22. Akta 680 – Aktiviti Kerajaan Elektronik 2007.
23. 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
24. 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.
25. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.
26. Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006.
27. Akta 658 – Akta Perdagangan Elektronik 2006.
28. Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam 29. Akta 629 – Akta Arkib Negara 2003. [
30. Akta 606 – Akta Cakera Optik 2000.
31. Akta 588 – Akta Komunikasi dan Multimedia 1998. (in revision)
32. Akta 562 - AktaTandatangan Digital 1997.
33. [Akta 563 – Akta Jenayah Komputer 1997.

34. Akta 564 - Telemedicine Act 1997. (not enforced)
35. Akta 88 – Akta Rahsia Rasmi 1972.
36. Akta 332 – Akta Hak Cipta 1987.
37. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).
38. Akta 298 – Kawasan Larangan Tempat Larangan 1959Akta 56 – Akta Keterangan 1950.
39. National Cyber Security Policy (NCSP)
40. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies /Organisations.
41. Arahan Tetap Sasaran Penting.
42. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
43. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
44. Perintah Am Bab D.