JABATAN AKAUNTAN NEGARA MALAYSIA

POLISI KESELAMATAN SIBER

PKS 2.0

POLISI KESELAMATAN SIBER

PKS 2.0

Diterbitkan oleh:
Bahagian Pengurusan Teknologi Maklumat (BPTM)
Jabatan Akauntan Negara Malaysia (JANM)
No 1, Persiaran Perdana, Presint 2, 62594 Putrajaya

E-mel: bptm@anm.gov.my
Telefon: 03-8882 1000
Laman web: www.anm.gov.my

Cetakan 2026

SEJARAH DOKUMEN

TAHUN	NAMA DOKUMEN	VERSI	KELULUSAN	TARIKH KUATKUASA
2019	Dasar Keselamatan ICT	5.1	JPICT JANM Bil.1/2019	25 Januari 2019 Sehingga 5 Julai 2022
2022	Polisi Keselamatan Siber	1.0	JPICT JANM Bil.3/2022	6 Julai 2022
2024	Polisi Keselamatan Siber	1.1	JPICT JANM Bil.4/2024	4 Julai 2024
2026	Polisi Keselamatan Siber	2.0	JPICT JANM Bil 2/2026	15 April 2026

ISI KANDUNGAN

PENGENALAN

Polisi Keselamatan Siber (PKS) Jabatan Akauntan Negara Malaysia (JANM) mengandungi peraturan-peraturan yang mesti dibaca, difahami dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) JANM. Dasar ini menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JANM. Dokumen ini hendaklah dibaca bersama dengan Garis Panduan Teknologi Maklumat dan Komunikasi (GPTMK) versi 2.0 yang merangkumi perkara berikut:

a. Akaun dan Capaian;

b. E-mel Rasmi;

c. Rangkaian dan Keselamatan;

d. Perkakasan dan Perisian;

e. Pengurusan Keselamatan Sistem Aplikasi;

f. Perkhidmatan Prasarana Kunci Awam (PKI);

g. Pengurusan Migrasi Kriptografi Pasca Kuantum (PQC); dan

h. Pihak Ketiga.

OBJEKTIF

PKS JANM diwujudkan untuk menjamin kesinambungan urusan JANM dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Polisi Keselamatan ICT JANM ialah seperti berikut:

a. Memastikan kelancaran operasi JANM dan meminimumkan kerosakan atau kemusnahan;

b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

c. Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

PKS JANM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

e. Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain daripada itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT JANM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS JANM menetapkan keperluan-keperluan asas berikut:

a. Data dan maklumat hendaklah boleh diakses secara berterusan dengan tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti;

b. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat; dan

c. Kaedah penghapusan rekod dan teknik penyamaran data yang selamat hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Garis Panduan Akauntan Negara Malaysia: Pelaksanaan Pengarkiban dan Dapatan Semula Rekod dan tatacara pelupusan oleh Jabatan Arkib Negara yang berkuatkuasa bagi mengelakkan pendedahan data sensitif dari akses yang tidak dibenarkan.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa,PKS JANM ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a **Perkakasan**

Semua aset yang digunakan untuk menyokong penyediaan, pemprosesan dan kemudahan storan maklumat JANM. Contoh komputer, *server*, peralatan komunikasi dan sebagainya;

b **Perisian**

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada JANM;

c **Perkhidmatan**

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d **Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif JANM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

e **Manusia**

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian JANM bagi mencapai misi dan objektif JANM. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f **Premis Komputer Dan Komunikasi**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a) - (e)** di atas.

Setiap perkara di atas perlu diberi perlindungan yang rapi. Sebarang kebocoran maklumat rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS JANM dan perlu dipatuhi adalah seperti berikut:

a **Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b **Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap akses yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat.

Hak akses perlu dikaji semula sebaik sahaja terdapat perubahan pada peranan, tanggungjawab atau bidang tugas pengguna;

c **Akauntabiliti**

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka;

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan
v. Memberi perhatian kepada maklumat terperingkat terutama semasa perwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

d **Pengasingan**

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

Aliran data bagi maklumat rasmi terperingkat hendaklah diasingkan daripada aliran Data Terbuka dan Maklumat Pengenalan Peribadi (*PII)*. Selain itu, aliran data bagi empat (4) kategori maklumat rasmi terperingkat hendaklah juga diasingkan.

e **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti tahap pematuhan terhadap PKS bagi mengawal insiden berkaitan dengan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan kesediaan aset ICT memelihara semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, *server*, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f **Pematuhan**

PKS JANM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g **Pemulihan**

Pemulihan sistem selepas berlaku gangguan atau kegagalan amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk memulihkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penyalinan semula penduaan (*restore backup*) dan mewujudkan pelan pemulihan bencana atau kesinambungan perkhidmatan; dan

h **Saling Bergantungan**

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan menyediakan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

BIDANG 01- POLISI KESELAMATAN MAKLUMAT

0101- Polisi Keselamatan Siber

BIDANG 01 POLISI KESELAMATAN MAKLUMAT

0101 Polisi Keselamatan Siber

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JANM dan perundangan yang berkaitan.

010101 Pelaksanaan Polisi

PERANAN: ANM

Pelaksanaan polisi ini akan dijalankan oleh Akauntan Negara Malaysia (ANM) selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) JANM. Ahli JPICT ini terdiri daripada Timbalan Akauntan Negara, Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian atau wakil ganti.

010102 Penyebaran Polisi

PERANAN: ICTSO

Polisi ini perlu disebarkan kepada semua pengguna JANM (termasuk kakitangan, pembekal, pakar runding dan lain-lain).

010103 Penyenggaraan Polisi

PERANAN: ICTSO

PKS JANM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial.

Berikut adalah prosedur yang berhubung dengan penyenggaraan PKS JANM:

a. Kenal pasti dan tentukan perubahan yang diperlukan;

b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat JPICT, JANM;

c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan

d. Dasar ini hendaklah dikaji semula sekurang-kurangnya tiga (3) tahun sekali atau mengikut keperluan semasa.

010104 Pengecualian Polisi

PERANAN: Pengguna

PKS JANM adalah terpakai kepada semua pengguna ICT JANM dan tiada pengecualian diberikan.

BIDANG 02 - PERANCANGAN BAGI KESELAMATAN ORGANISASI

0201- Infrastruktur Organisasi Dalaman

0202- Peralatan Mudah Alih dan Kerja Jarak Jauh

BIDANG 02 PERANCANGAN BAGI KESELAMATAN ORGANISASI

0201 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS JANM.

020101 Akauntan Negara Malaysia

PERANAN: ANM

Struktur Organisasi Pengurusan Keselamatan ICT JANM diberikan seperti di **Lampiran 1** ANM adalah berperanan dan bertanggungjawab dalam perkara-perkara berikut:

a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah PKS JANM;

b. Memastikan semua pengguna mematuhi PKS JANM;

c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;

d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS JANM;

e. Melantik CDO serta memaklumkan pelantikan kepada Ketua Pengarah, Jabatan Digital Negara (JDN); dan

f. Mempengerusikan Mesyuarat JPICT JANM.

020102 Ketua Pegawai Digital (CDO)

PERANAN: CDO

CDO bagi JANM ialah Timbalan Akauntan Negara (Korporat).

Peranan dan tanggungjawab CDO adalah seperti berikut:

a. Membantu ANM dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;

b. Menentukan keperluan keselamatan ICT;

c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan PKS JANM serta pengurusan risiko dan pengauditan;

d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT JANM;

e. Pengarah Pemulihan (*Recovery Director*) pengurusan kesinambungan perkhidmatan JANM;

f. Mengetuai Pasukan Tindak Balas Insiden Keselamatan ICT JANM (CSIRT JANM);

g. Melantik ICTSO serta memaklumkan pelantikan kepada JDN dan National Cyber Security Agency (NACSA); dan

h. Memastikan kakitangan JANM dan Pihak Ketiga memahami dan mematuhi peruntukan di bawah PKS.

020103 Pegawai Keselamatan ICT (ICTSO)

PERANAN: ICTSO

ICTSO bagi JANM ialah Pengarah Bahagian Pengurusan Teknologi Maklumat, JANM.

Peranan dan tanggungjawab ICTSO adalah seperti berikut:

a. Menyelaras keseluruhan program-program keselamatan ICT JANM seperti penyediaan PKS JANM, pengurusan risiko, melaksanakan program kesedaran keselamatan ICT dan pengauditan;

b. Menguatkuasakan pelaksanaan PKS JANM;

c. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS JANM;

d. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

e. Mengurus CSIRT JANM;

f. Melaporkan insiden keselamatan ICT kepada CDO bagi insiden yang memerlukan pengaktifan Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) JANM;

g. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

h. Menjalankan pengurusan risiko dan audit keselamatan ICT JANM berpandukan peraturan dan garis panduan yang berkuatkuasa;

i. Menyemak laporan berkaitan dengan isu-isu keselamatan ICT; dan

j. Mempengerusikan Mesyuarat Jawatankuasa Kerja Keselamatan ICT JANM.

020104 Pengurus ICT

PERANAN: Pengurus ICT

Pengurus-pengurus ICT bagi JANM ialah Pengarah Bahagian, Pengarah JANM Negeri dan Pengarah JANM Cawangan.

a. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JANM;

c. Menentukan kawalan akses pengguna terhadap aset ICT JANM;

d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan

e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JANM.

020105 Pentadbir ICT

PERANAN: Pentadbir ICT

Pentadbir ICT bagi JANM ialah Ketua bagi pentadbiran perkakasan dan perisian, aplikasi, rangkaian dan keselamatan ICT, pusat data, pangkalan data dan e-mel.

Peranan dan tanggungjawab Pentadbir ICT adalah seperti berikut:

a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, berlaku perubahan dalam bidang tugas, bercuti atau berkursus panjang;

b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam PKS JANM;

c. Memantau aktiviti capaian harian sistem ICT;

d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta, serta memaklumkan kepada ICTSO atau Pengurus ICT;

e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO, CDO dan Ahli Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (CS) dengan segera;

f. Menganalisis dan menyimpan rekod jejak audit;

g. Bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik;

h. Menyediakan khidmat nasihat ICT (Kejuruteraan Keperluan Sistem dan kejuruteraan Pembangunan Sistem):

   i. Pembangunan Sistem
   ii. Infrastruktur ICT
   iii. Rangkaian dan Keselamatan ICT; dan
   iv. Penyenggaraan Sistem.

i. Memastikan, menyemak dan memantau sistem sokongan yang dibangunkan.

020106 Pentadbir Perkakasan Dan Perisian

PERANAN: Pentadbir Perkakasan dan Perisian

Pentadbir Perkakasan dan Perisian mempunyai tanggungjawab seperti berikut:

a. Menguruskan akaun pentadbir atau pengguna bagi perkakasan dan perisian/sistem operasi yang berkaitan;

b. Mengurus perkakasan dan perisian berdasarkan kepada polisi yang telah ditetapkan dalam PKS dan GPTMK;

c. Memastikan konfigurasi perkakasan dan perisian yang selamat dilaksanakan; dan

d. Membuat pemantauan dan penyenggaraan ke atas prestasi dan keselamatan perkakasan dan perisian secara berkala.

020107 Pentadbir Aplikasi dan Pangkalan Data

PERANAN: Pentadbir Aplikasi dan Pangkalan Data

Pentadbir Aplikasi dan angkalan Data mempunyai tanggungjawab seperti berikut:

a. Menguruskan pendaftaran akaun pentadbir atau pengguna bagi aplikasi atau pangkalan data yang berkaitan;

b. Mengurus sistem aplikasi atau pangkalan data berdasarka kepada polisi yang telah ditetapkan di dalam PKS dan GPTMK;

c. Memastikan konfigurasi pangkalan data yang selamat dilaksanakan; dan

d. Membuat pemantauan dan penyenggaraan ke atas prestasi dan keselamatan aplikasi atau pangkalan data secara berkala.

020108 Pentadbir Rangkaian dan Keselamatan

PERANAN: Pentadbir Rangkaian dan Keselamatan

Pentadbir Rangkaian dan Keselamatan mempunyai tanggungjawab seperti berikut:

a. Menguruskan pendaftaran akaun pentadbir atau pengguna bagi rangkaian dan keselamatan ICT yang berkaitan;

b. Menentukan rangkaian dan keselamatan berdasarkan kepada polisi yang telah ditetapkan dalam PKS dan GPTMK;

c. Memastikan polisi atau konfigurasi yang selamat dilaksanakan;

d. Membuat pemantauan dan penyenggaraan ke atas prestasi dan keselamatan rangkaian dan keselamatan ICT secara berkala; dan

e. Melaporkan insiden perlanggaran keselamatan rangkaian dan keselamatan kepada pasukan CSIRT JANM.

020109 Pentadbir E-mel

PERANAN: Pentadbir E-mel

Pentadbir E-mel mempunyai tanggungjawab seperti berikut:

a. Menguruskan pendaftaran akaun pengguna e-mel bagi warga JANM;

b. Memastikan polisi atau konfigurasi e-mel yang selamat dilaksanakan;

c. Membuat pemantauan ke atas prestasi dan keselamatan sistem e-mel;

d. Mengurus konfigurasi e-mel berdasarkan kepada polisi yang telah ditetapkan di dalam PKS dan GPTMK; dan

e. Melaporkan kepada pihak JDN sekiranya berlaku insiden yang berkaitan.

020110 Pengguna

PERANAN: Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut:

a. Membaca, memahami dan mematuhi PKS JANM;

b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;

c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;

d. Melaksanakan prinsip-prinsip PKS JANM dan menjaga kerahsiaan maklumat JANM;

e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada pentadbir sistem dengan segera;

f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan

g. Pengesahan Surat Akuan Pematuhan PKS JANM sebagaimana **Lampiran 2** (secara atas talian).

020111 Jawatankuasa Pemandu ICT JANM

PERANAN: JPICT

JPICT bertanggungjawab dalam merancang dan menentukan langkah-langkah keselamatan siber JANM seperti yang terkandung dalam Surat Pekeliling Am Bil 7 Tahun 2024.

a. JPICT bertanggungjawab menetapkan arah hala tuju, strategi dan perancangan program keselamatan ICT JANM.

Bidang kuasa JPICT berkaitan Keselamatan ICT:

i. Meluluskan dasar dan aktiviti keselamatan ICT JANM

ii.

Keanggotaan JPICT JANM adalah seperti berikut:

Pengerusi: Y.Bhg. Akauntan Negara Malaysia.

Ahli-ahli:

1. Timbalan Akauntan Negara Operasi (O).
2. Timbalan Akauntan Negara Korporat (K) (CDO).
3. Pengarah BPTM (ICTSO).
4. Semua Pengarah Bahagian.

Urus Setia bagi JPICT ialah Bahagian Pengurusan Teknologi Maklumat (BPTM) Seksyen Kualiti dan Perancangan (SKP).

020112 Jawatankuasa Keselamatan ICT JANM

PERANAN: JKICT

JKICT adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT JANM.

Bidang kuasa JKICT:

i. Memperaku dasar dan ktiviti keselamatan ICT JANM;
ii. Memperaku cadangan pengemaskinian dan memantau pelaksanaan PKS; dan
iii. Memperaku perancangan Program Keselamatan ICT dan Program Penilaian Tahap Keselamatan (PTK) ICT.

Keanggotaan JKICT JANM adalah seperti berikut:

Pengerusi: Timbalan Akauntan Negara Korporat (K) (CDO).

Ahli:

1. Pengarah BPTM (ICTSO).
2. Wakil Timbalan Pengarah Bahagian yang dilantik.

Urus Setia bagi JKICT JANM ialah Bahagian Pengurusan Teknologi Maklumat (BPTM), Unit Pengurusan Rangkaian dan Keselamatan ICT (URK).

020113 Jawatankuasa Kerja Keselamatan ICT JANM

PERANAN: JKKICT

Jawatankuasa Kerja Keselamatan ICT (JKKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT JANM.

Bidang kuasa JKKICT:

i. Merancang Dasar, Strategi dan Pelan Tindakan Keselamatan ICT;
ii. Merancang, mencadang pengemaskinian dan memantau pelaksanaan PKS; dan
iii. Merancang dan melaksana Program Keselamatan ICT.
iv. Merancang, melaksana dan memantau Program Penilaian Tahap Keselamatan (PTK) ICT.

Keanggotaan JKKICT JANM adalah seperti berikut:

Pengerusi : Pengarah BPTM (ICTSO).

Ahli-Ahli:

1. Semua Timbalan Pengarah BPTM.
2. Ketua Penolong Pengarah (K) BPTM.

3. Ketua Penolong Pengarah BPTM.
4. Pegawai Teknikal Bahagian atau Pentadbir Sistem.
5. Ketua Unit atau Modul Bahagian.

Urus Setia bagi JKKICT JANM ialah Bahagian Pengurusan Teknologi Maklumat (BPTM), Unit Pengurusan Rangkaian dan Keselamatan ICT (URK).

020114 Pasukan Tindak Balas Insiden Keselamatan ICT

PERANAN: CSIRT JANM

Ahli-ahli CSIRT JANM yang dilantik daripada BPTM JANM adalah merupakan ahli CSIRT Kementerian Kewangan (MOF).

Peranan dan tanggungjawab CSIRT adalah seperti berikut:

a. Mengesan atau menerima aduan insiden keselamatan ICT dan menilai tahap serta jenis insiden;
b. Merekod dan menjalankan siasatan awal insiden yang diterima;
c. Melaporkan insiden kepada ICTSO JANM;
d. Menangani insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;
e. Mengesyorkan JANM mengambil tindakan pemulihan dan pengukuhan; dan
f. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada JANM.

020115 Pemilik Sistem

PERANAN: Pemilik Sistem

Tanggungjawab Pemilik Sistem adalah seperti berikut:

a. memastikan aplikasi mematuhi PSP serta mengikut pekeliling semasa yang berkuat kuasa;

b. memastikan kesesuaian teknologi dan ciri-ciri keselamatan yang perlu ada bagi aplikasi;

c. memastikan kelancaran operasi sistem dengan meminimumkan risiko keselamatan berkaitan dengan aplikasi.

d. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu;

e. pembelian atau peningkatan perisian dan sistem komputer;

f. perolehan teknologi dan perkhidmatan komunikasi baharu;

g. pelantikan pembekal, perunding atau rakan usaha sama;

h. menentukan pembekal, perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan; dan

i. melaporkan insiden perlanggaran polisi keselamatan kepada pasukan CSIRT JANM.

020116 Pegawai Aset

PERANAN: Pegawai Aset

Tanggungjawab Pegawai Aset adalah seperti berikut:

a. Mengurus aset mengikut peraturan yang telah ditetapkan; dan

b. Menyediakan laporan pengurusan aset.

020117 Pengasingan Tugas dan Tanggungjawab

PERANAN: Pengurus ICT dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Skop tugas dan tanggungjawab perlu diasingkan mengikut skop kerja yang ditetapkan bagi mengelak penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aser ICT.

020118 Pengendali

PERANAN: Pengendali

Tanggungjawab Pengendali adalah seperti berikut:

a. Mengurus pengendalian aset; dan

b. Mengurus pengendaliaan media.

0202 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

020201 Peralatan Mudah Alih

PERANAN: Pengguna

Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti tablets, *Personal Digital Assistances* (PDA), telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu *Universal Serial Bus* (USB) atau lain-lain peralatan yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik.

Pelaksanaan langkah-langkah kawalan perlindungan bagi komputer riba dan peranti mudah alih adalah seperti berikut:

a. Semua pengguna bertanggung jawab sepenuhnya terhadap pengurusan dan kawalan keselamatan setiap komputer riba dan peranti mudah alih yang dibekalkan. Rekod penggunaan hendaklah diwujudkan, dikemaskini dan diperiksa;

b. Memastikan komputer riba dan peranti mudah alih dihindari daripada sebarang ancaman, keselamatan maklumat seperti pendedahan, kecurian, pengubahsuaian dan pemalsuan;

c. Peralatan dibawa keluar bagi tujuan rasmi termasuk yang mengandungi maklumat rahsia rasmi hendaklah mendapat kebenaran secara bertulis daripada Ketua Jabatan selaras dengan Arahan Keselamatan dan Pekeliling semasa yang berkuatkuasa;

d. Komputer riba dan peranti mudah alih tidak digunakan untuk menyimpan maklumat rahsia rasmi. Sekiranya ada keperluan untuk berbuat demikian, maklumat rahsia rasmi hendaklah dienkrip;

e. Komputer riba atau peranti mudah alih semasa tidak digunakan hendaklah disimpan di dalam bekas-bekas keselamatan atau di dalam bilik berkunci;

f. Komputer riba dan peranti mudah alih tidak disimpan di dalam kenderaan tanpa pengawasan, di tempat-tempat awam dan premis atau kawasan yang tidak selamat;

g. Komputer riba dan peranti mudah alih yang dibawa menaiki pesawat dan kenderaan awam hendaklah sentiasa berada di dalam simpanan dan kawalan selamat pengguna;

h. Komputer riba dan peranti mudah alih yang didapati hilang hendaklah dilaporkan oleh Ketua Jabatan atau Pegawai Keselamatan Jabatan atau CDO kepada Polis Diraja Malaysia (PDRM) dan satu salinan laporan siasatan hendaklah dikemukakan kepada Ketua Pengarah Kerajaan Malaysia. Komputer riba dan peranti mudah alih yang hilang dan dipercayai mengandungi maklumat rahsia rasmi hendaklah dibuat taksiran bahaya. Sekiranya kehilangan maklumat rahsia rasmi disahkan, Kementerian, Jabatan, Agensi Kerajaan yang terlibat hendaklah dihubungi supaya tindakan pembetulan dapat diambil; dan

i. Jika komputer riba dan peranti mudah alih yang mengandungi maklumat rahsia rasmi terbukti hilang, Ketua Jabatan hendaklah menimbang dan mengambil tindakan tatatertib atau penyiasatan dan pendakwaan di bawah Akta Rahsia Rasmi 1972.

020202 Kerja Jarak Jauh

PERANAN: Pengguna

Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan, pendedahan dan capaian maklumat tidak sah atau salah guna.

a. Penghantaran maklumat rasmi dengan capaian jarak jauh mestilah menggunakan kaedah penyulitan (*encryption*).

b. Penggunaan perkhidmatan untuk tugas rasmi secara jarak jauh hendaklah mendapat kebenaran daripada CDO, ICTSO, Pengurus ICT atau Pentadbir ICT.

BIDANG 03 - KESELAMATAN SUMBER MANUSIA

0301 - Keselamatan Sumber Manusia Dalam Tugas Harian

BIDANG 03 KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk warga JANM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga JANM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

030101 Sebelum Perkhidmatan

PERANAN: Pengguna

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a. Memahami dengan jelas peranan dan tanggungjawab warga JANM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;

b. Memastikan tapisan keselamatan dijalankan untuk warga JANM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan

c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

030102 Dalam Perkhidmatan

PERANAN: Semua

Perkara-perkara perlu dipatuhi termasuk yang berikut:

a. Memastikan warga JANM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT mengikut perundangan dan peraturan yang ditetapkan oleh JANM;

b. Memastikan latihan kesedaran yang berkaitan pengurusan keselamatan aset ICT diberi kepada pengguna ICT JANM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;

c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga JANM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh JANM; dan

d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT, bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.

030103 Bertukar Atau Tamat Perkhidmatan

PERANAN: Pengguna

Perkara-perkara perlu dipatuhi termasuk yang berikut:

a. Memastikan semua aset ICT dikembalikan kepada JANM mengikut peraturan atau terma perkhidmatan yang ditetapkan;

b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh JANM atau terma perkhidmatan; dan

c. Membatalkan atau nyahaktif (*disable*) semua capaian ke atas sistem, perkakasan dan perisian mengikut peraturan yang ditetapkan oleh JANM serta pekeliling semasa yang berkuat kuasa.

030104 Kompetensi Warga JANM

PERANAN: Warga JANM

Kompetensi warga JANM termasuk:

a. Mewujudkan komunikasi ICT dan program kesedaran bagi amalan terbaik keselamatan ICT;

b. Latihan kemahiran menggunakan peralatan ICT yang mencukupi hendaklah diberikan kepada warga JANM bagi memastikan mereka mampu melaksanakan tugasan harian; dan

c. Kompetensi ICT tambahan hendaklah diberikan kepada warga JANM yang diberi kuasa mengendalikan dokumen terperingkat selaras dengan arahan pekeliling semasa.

Kompetensi warga JANM yang menguruskan aset ICT hendaklah memenuhi kompetensi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

BIDANG 04- PENGURUSAN ASET

0401- Akauntabiliti Aset

0402- Pengelasan dan Pengendalian Maklumat

0403- Pengurusan Media

BIDANG 04 PENGURUSAN ASET

0401 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JANM.

040101 Inventori Aset ICT

PERANAN: Warga JANM

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Memastikan semua maklumat aset ICT direkodkan dalam daftar harta modal dan inventori serta sentiasa dikemas kini;

   i. Peralatan pengguna yang dibenarkan (contoh: laptop, desktop, *tablet*)
   ii. Peralatan rangkaian (contoh: *switch, firewall, router, wireless access point*)
   iii. Peralatan *Internet of Things (IoT)* (contoh*: printer, smart television)*
   iv. Server (contoh: server aplikasi, server web)
   v. Perisian melalui perolehan Jabatan kecuali perisian langganan (contoh: *operating system,* pangkalan data, aplikasi)

b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja serta maklumat pendaftaran mesti mengandungi;

   i. Nombor pengenalan yang unik
   ii. Tarikh Perolehan
   iii. Harga perolehan/Nilai aset
   iv. Jenis dan kategori
   v. Maklumat Pengeluar

vi. Model atau Nombor siri
vii. Lokasi yang ditempatkan
viii. Maklumat pemilik aset

c. Memastikan semua pengguna mengesahkan penempatan aset ICT dimiliki dan ditempatkan di JANM;

d. Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan;

e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

f. Rekod aset ICT hendaklah disemak secara berkala dan/atau apabila berlaku sebarang perubahan, seperti perolehan sistem baharu atau *decommisioning* aset lama. Pengesahan perlu dilaksanakan terhadap perkara berikut:

i. Pemilikan aset
ii. Status aset (contohnya: sedang digunakan, tidak digunakan, rosak, dalam penyelenggaraan, dipinjam, hilang dan sebagainya)
iii. Pelupusan aset
iv. Kesahihan lesen perisian

040102 Pindah Hak Milik

PERANAN: Warga JANM

Pemindahan hak milik aset berlaku dalam keadaan berikut:

a. Pekerja meninggalkan Jabatan disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

b. Aset yang dikongsi untuk kegunaan sementara;

c. Pemberian aset kepada Jabatan lain; dan

d. Aset dikembalikan setelah tamat tempoh sewaan.

Data dalam peranti tersebut hendaklah diuruskan sepertimana pelupusan perkakasan.

040103 Penyenggaraan Aset ICT

PERANAN: Warga JANM

Aset ICT hendaklah dijaga dan rekod dikemaskini secara berterusan untuk menggambarkan:

a. Aset perolehan baharu

b. Aset yang *decommissioned* atau dilupuskan

c. Kesahihan lesen perisian

d. Perubahan pemilik atau lokasi yang ditempatkan

0402 Pengelasan dan Pengendalian Maklumat

Objektif:

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

040201 Pengelasan Maklumat

PERANAN: Pengguna

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen.

Arahan Keselamatan seperti berikut:

a. Rahsia Besar;

b. Rahsia;

c. Sulit; atau

d. Terhad.

PII adalah maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi serta data sensitif individu dan ianya juga terkandung dalam Maklumat Rahsia Rasmi.

040202 Pengendalian Maklumat

PERANAN: Pengguna

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar, menyamar *(data masking*), menghapus dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

a. Menghalang pendedahan dan ketirisan maklumat kepada pihak yang tidak dibenarkan;
b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
c. Menentukan maklumat sedia untuk digunakan;
d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
e. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
f. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

0403 Pengurusan Media

Objektif:

Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

040301 Penghantaran dan Pemindahan

PERANAN: Warga JANM

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.

040302 Prosedur Pengendalian Media

PERANAN: Warga JANM

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:

a. Melabelkan semua media mengikut kandungan dan disimpan ditempat yang sesuai dan selamat;

b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

d. Mengawal dan merekodkan aktiviti menyenggara media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan

e. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah mengikut prosedur pelupusan semasa.

040303 Pelupusan Perkakasan

PERANAN: Warga JANM

Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT JANM dilupuskan dengan teratur iaitu:

a. Peralatan akan ditentukan oleh kakitangan ICT berkaitan sama ada boleh dilupuskan atau sebaliknya;

b. Pelupusan hendaklah dilakukan mengikut tatacara pelupusan kerajaan berdasarkan pekeliling yang berkuat kuasa;

c. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal

d. Pelupusan data dan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara pelupusan oleh Jabatan Arkib Negara yang berkuatkuasa.

BIDANG 05- KAWALAN CAPAIAN

0501- Kawalan Capaian

0502- Pengurusan Capaian Pengguna

0503- Tanggungjawab Pengguna

0504- Kawalan Capaian Rangkaian

0505- Kawalan Capaian Sistem Pengoperasian

0506- Kawalan Capaian Aplikasi dan Maklumat

BIDANG 05 KAWALAN CAPAIAN

0501 Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat.

050101 Keperluan Kawalan Capaian

PERANAN: ICTSO

Kawalan capaian perlu disedia, didokumen dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Capaian kepada pemprosesan dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

Tahap capaian perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Mengawal capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna;

b. Mengawal capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

c. Mengawal keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan

d. Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam elemen persekitaran pengkomputeran yang disahkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).

0502 Pengurusan Capaian Pengguna

Objektif:

Memastikan capaian pengguna yang dibenarkan melalui pengenalan pengguna dan menghalang capaian pengguna yang tidak dibenarkan ke atas sistem maklumat.

Pengenalan pengguna hendaklah merujuk kepada seorang pengguna sahaja. Capaian pengenalan pengguna kepada personel Sektor Awam hendaklah tertakluk kepada proses pengesahan yang ketat.

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

050201 Akaun Pengguna

PERANAN: Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan dan perlu mempunyai akaun pengguna masing-masing bagi mencapai sistem ICT. Akaun yang telah diwujudkan hendaklah mematuhi perkara-perkara berikut:

a. Mengawal pewujudan akaun kepada pengguna yang dibenarkan dan mencerminkan identiti pengguna serta bidang tugas yang diperuntukkan sahaja;

b. Mendapatkan kelulusan pemilik sistem ICT bagi pewujudan akaun pengguna;

c. Membatalkan pemilikan akaun pengguna yang melanggar peraturan atau mengikut keperluan; dan

d. Bagi aplikasi yang mengandungi Maklumat Rahsia Rasmi dan PII, pengesahan pengguna hendaklah berdasarkan lebih daripada satu faktor pengenalan pengguna mengikut kaedah yang bersesuaian seperti *multi-factor authentication (MFA)*.

050202 Hak Capaian

PERANAN: Pentadbir ICT

Pewujudan capaian hak istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

050203 Pengurusan Kata Laluan

PERANAN: Pengguna

Pemilihan, penggunaan, penukaran dan pengurusan kata laluan bagi mencapai sistem ICT mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan agar kata laluan tidak terdedah kepada orang lain. Penggunaan kata laluan asal (*default*) untuk perkakasan dan perisian adalah tidak dibenarkan dalam persekitaran sebenar.

050204 Semakan Capaian Pengguna

PERANAN: Pentadbir ICT

Hak capaian pengguna hendaklah dikaji dari semasa ke semasa melalui saluran yang ditetapkan.

0503 Tanggungjawab Pengguna

Objektif:

Maklumat dan kemudahan pemprosesan maklumat hendaklah dihalang daripada penyalahgunaan, kecurian atau capaian oleh pengguna yang tidak dibenarkan.

050301 Penggunaan Kata Laluan

PERANAN: Pengguna

Amalan terbaik dalam pemilihan dan penggunaan kata laluan hendaklah dipatuhi oleh pengguna.

050302 Peralatan Tanpa Kehadiran Pengguna (*Unattended User Equipment*)

PERANAN: Pengguna

Peralatan ICT yang hendak ditinggalkan atau ditamatkan penggunaannya hendaklah diberi perlindungan yang bersesuaian atau ditamatkan sesinya (*logout, switch off* atau *logoff)* bagi mengelakkan capaian yang tidak dibenarkan.

050303 *Clear Desk* dan *Clear Screen*

PERANAN: Pengguna

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan maklumat rasmi yang terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;

b. Menyimpan maklumat rasmi di dalam laci atau kabinet yang berkunci; dan

c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin *faksimile* dan mesin fotostat.

050304 Peranti Pengkomputeran Peribadi (*Bring Your Own Devices*, BYOD)

PERANAN: Pengguna

BYOD merupakan peralatan mudah alih persendirian seperti komputer riba, komputer tablet atau telefon pintar yang digunakan untuk mengakses kepada maklumat JANM. Pengguna yang menggunakan kemudahan rangkaian JANM dan MyGovNet/PCN atau *data line* persendirian untuk akses maklumat JANM tertakluk kepada PKS, GPTMK JANM dan pekeliling berkaitan yang sedang berkuat kuasa.

Pengguna bertanggungjawab untuk mematuhi langkah-langkah keselamatan perlindungan berkaitan penggunaan BYOD seperti berikut:

a. mengelak risiko kebocoran maklumat rasmi;

b. mengelakkan ancaman risiko keselamatan ICT;

c. memelihara integriti data; dan

d. memastikan produktiviti pengguna tidak terjejas dalam menjalankan urusan rasmi jabatan.

Mekanisme kawalan hendaklah diwujudkan bagi mengawal dan memantau pelaksanaan BYOD adalah seperti berikut:

a. mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan; dan

b. memastikan peralatan BYOD bebas daripada sebarang *malware* dan ancaman keselamatan.

Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD.

Peranti Pengkomputeran Peribadi merangkumi perkara berikut:

a. Penggunaan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah mendapat kebenaran daripada JANM; dan

b. Peranti pengkomputeran peribadi dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat.

0504 Kawalan Capaian Rangkaian

Objektif:

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

050401 Capaian Rangkaian

PERANAN: Pentadbir ICT dan ICTSO

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan mematuhi perkara-perkara berikut:

a. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan

b. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

050402 Infrastruktur Rangkaian

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin untuk melindungi ancaman pada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara seperti berikut mestilah dipatuhi:

a. Rekabentuk infrastruktur rangkaian perlu mempunyai ciri-ciri keselamatan terbaik dari segi tahap keselamatan dengan dilindungi oleh mekanisme keselamatan rangkaian;

b. Menempatkan atau memasang peranti rangkaian yang bersesuaian di antara rangkaian setempat JANM, rangkaian luaran dan rangkaian terbuka;

c. Pemantauan rangkaian perlu dilakukan sepanjang masa untuk memastikan keselamatan rangkaian dengan mematuhi amalan terbaik serta prosedur yang ditetapkan; dan

d. Peranti milik persendirian yang digunakan untuk mencapai Maklumat Rasmi hendaklah didaftarkan dan dilarang sama sekali dibawa masuk ke kawasan larangan untuk mencapai Maklumat Rahsia Rasmi.

050403 Capaian Internet

PERANAN: Pentadbir Rangkaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pemantauan secara berterusan ke atas penggunaan internet JANM hendaklah dilakukan;

b. Penggunaan internet hanyalah untuk kegunaan rasmi dan terhad untuk tujuan yang dibenarkan sahaja;

c. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya tertakluk kepada peraturan yang ditetapkan;

d. Maklumat atau data yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber internet hendaklah dinyatakan; dan

e. Maklumat rasmi yang hendak dimuat naik perlu disemak dan mendapat pengesahan daripada pegawai yang bertanggungjawab sebelum dimuat naik ke internet.

0505 Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

050501 Capaian Sistem Pengoperasian

PERANAN: Pentadbir ICT dan ICTSO

Kawalan capaian sistem pengoperasian adalah perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem pengoperasian perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi:

a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan

b. Merekodkan capaian yang berjaya dan gagal.

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut:

a. Mengesahkan pengguna yang dibenarkan;

b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan

c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;

b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;

c. Menghadkan dan mengawal penggunaan perisian; dan

d. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

0506 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

050601 Capaian Aplikasi dan Maklumat

PERANAN: Pentadbir Perkakasan dan Perisian, Pentadbir Aplikasi, Pentadbir Rangkaian dan Keselamatan ICT

Bertujuan melindungi sistem aplikasi dan maklumat daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

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

a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut peranan yang telah ditetapkan;

b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*sistem log*);

c. Capaian kepada kod sumber aturcara (*programme source code)* hendaklah dihadkan;

d. Capaian sistem maklumat dan aplikasi secara jarak jauh dihad kepada perkhidmatan yang dibenarkan;

e. Penggunaan teknologi *Video Conferencing* yang memerlukan sumber jalur lebar yang tinggi (*high bandwidth*) perlu dihadkan pada masa tertentu sahaja;

f. Pengguna dan Pembekal/kontraktor penyenggaraan yang memerlukan akaun bagi mendapat capaian ke sistem-sistem di JANM perlu mendapatkan kebenaran daripada Pentadbir yang berkaitan; dan

g. Pengguna dan Pembekal atau kontraktor penyenggaraan bertanggungjawab untuk memaklumkan Pentadbir yang berkaitan sekiranya tidak memerlukan akaun lagi bagi tujuan capaian kepada sistem.

050602 Kawalan Capaian Perbankan Internet

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Melindungi sistem Perbankan Internet (*online banking*) daripada sebarang bentuk capaian yang tidak dibenarkan termasuk pencerobohan, pemalsuan identiti, kecurian maklumat dan apa jua jenayah siber.

Perbankan Internet merupakan sebarang bentuk transaksi dan pertukaran maklumat kewangan melalui internet yang melibatkan agensi kerajaan, swasta dan bank. Bagi memastikan kawalan capaian Perbankan Internet adalah kukuh, perkara-perkara berikut hendaklah dipatuhi:

a. Mewujudkan satu capaian yang selamat bagi pelaksanaan Perbankan Internet; dan

b. Peralatan keselamatan hendaklah dipasang di antara *host* Perbankan Internet dengan sistem JANM berkaitan bagi tujuan pemantauan dan keselamatan.

050603 Pengkomputeran Awan *(Cloud Computing)*

PERANAN: Pengguna

a. Teknologi pengkomputeran awan yang bergantung kepada sumber pengkomputeran seperti pelayan, storan, pangkalan data, rangkaian dan perisian yang boleh dicapai menerusi rangkaian atau Internet;

b. Pengkomputeran awan hendaklah dipastikan selamat selaras dengan Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam yang telah disediakan oleh kerajaan; dan

c. Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak pengurusan.

BIDANG 06- KRIPTOGRAFI

0601- Kawalan Kriptografi

BIDANG 06 KRIPTOGRAFI

0601 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti, *non-repudiation* dan kesahihan maklumat elektronik melalui kawalan kriptografi.

060101 Enkripsi

PERANAN: Pengguna

a. Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

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

060102 Tandatangan Digital

PERANAN: Pengguna

Penggunaan tandatangan digital dimestikan kepada pengguna yang melaksanakan transaksi maklumat rahsia rasmi.

060103 Pengurusan Prasarana Kunci Awam (PKI)

PERANAN: Pentadbir ICT

a. PKI yang digunakan hendaklah dikeluarkan oleh pihak berkuasa pensijilan digital Malaysia yang sah sahaja;

b. Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; dan

c. Token adalah perkakasan yang mengandungi cip kriptografi untuk menyimpan sijil digital bagi melaksanakan fungsi Prasarana Kunci Awam.

060104 Prasarana Kunci Awam (PKI)

PERANAN: Pengguna

Public Key Infrastructure (PKI) atau Prasarana Kunci Awam adalah gabungan perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan komunikasi dan transaksi urus niaga dalam internet. PKI membolehkan pengguna melakukan transaksi secara elektronik dengan selamat serta mengenal pasti seseorang individu yang melakukan transaksi.

a. Kaedah yang selamat hendaklah digunakan bagi melindungi komunikasi rangkaian, seperti *Secure Socket Layer* (SSL) atau *Virtual Private Network* (VPN);

b. Bagi melakukan transaksi selamat, PKI seperti *token* merupakan satu kemudahan bagi menjamin integriti data yang dihasilkan melalui sistem aplikasi menggunakan kaedah pengesahan pengenalan identiti pengguna semasa tandatangan digital; dan

c. ID Sijil digital pengguna adalah sama dengan pengenalan identiti yang telah disemak silang dengan sistem JPN.

Penggunaan PKI perlu mematuhi perkara-perkara seperti berikut:

a. Pemegang sijil digital pengguna hendaklah merahsiakan ID dan Nombor PIN serta tidak dikongsi dengan pihak lain;

b. Token hendaklah digunakan bagi capaian dan tandatangan digital ke atas sistem yang dikhususkan sahaja mengikut peranan atau tahap kelayakan;

c. Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;

d. Akta Tandatangan Digital 1997 tidak membenarkan sijil digital pengguna untuk dipindah milik kerana sijil digital tersebut merupakan identiti pengguna dalam ruang *cyber*;

e. Perkongsian Token untuk sebarang capaian dan tandatangan digital sistem adalah tidak dibenarkan sama sekali;

f. Sebarang kehilangan, kerosakan dan kata laluan yang disekat perlu dimaklumkan kepada Pentadir portal GPKI; dan

g. Pemegang sijil digital perlu memulangkan token apabila tamat perkhidmatan, bersara atau tidak digunakan dalam sistem kepada agensi pusat menerusi pentadbir portal GPKI.

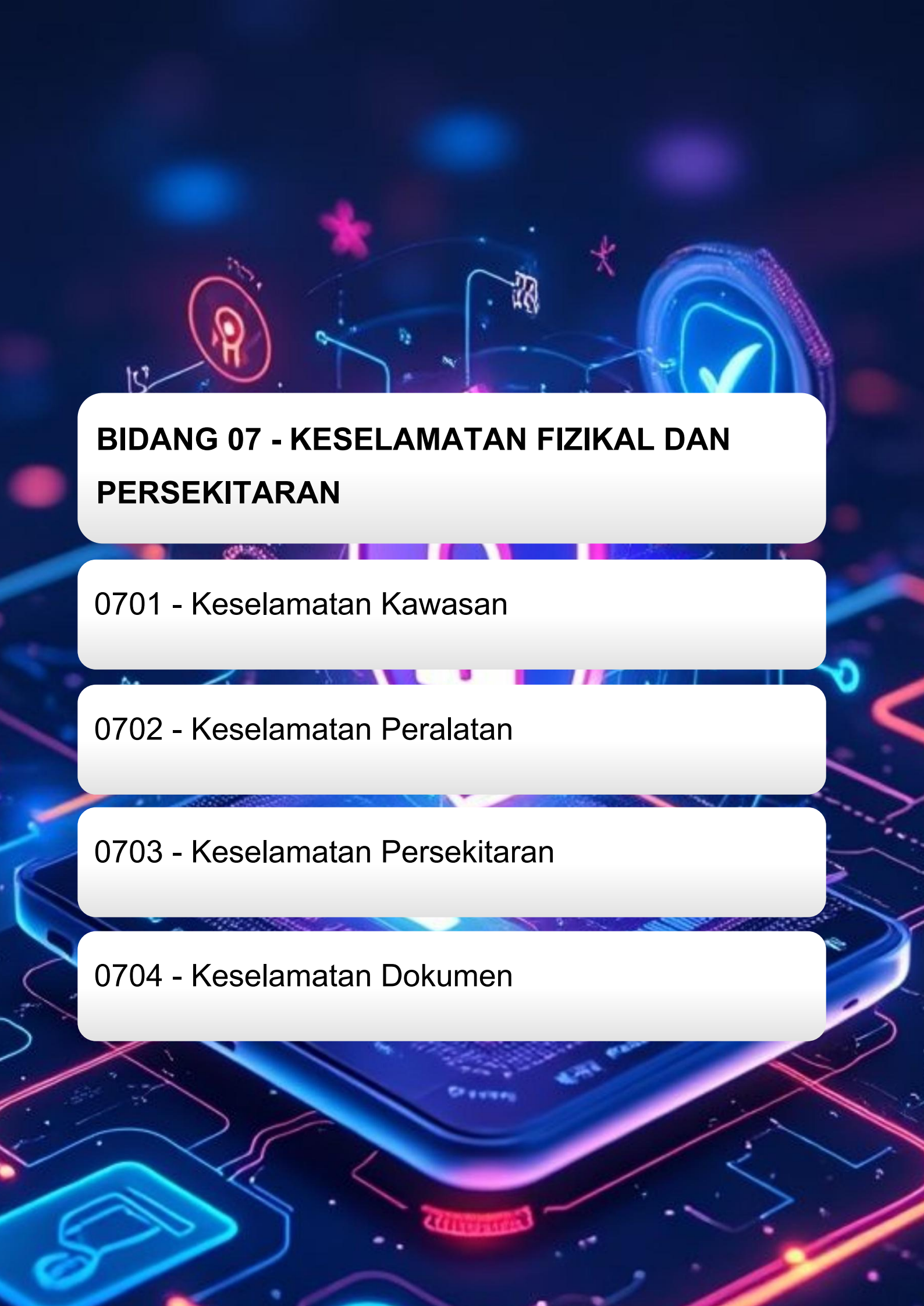
060105 Kriptografi Pasca Kuantum (*Post-Quantum Cryptography*, PQC)

PERANAN: Pengurus ICT, Pentadbir ICT dan Pemilik Sistem

PQC adalah kaedah penyulitan dan tandatangan digital yang direka untuk melindungi data, komunikasi, dan sistem ICT daripada ancaman komputer kuantum pada masa hadapan. PQC melindungi transaksi digital kritikal dan maklumat sensitif, serta memastikan keselamatan jangka panjang tanpa memerlukan perisian kuantum. Pengurus ICT dan Pentadbir ICT perlu:

a. Meningkatkan tahap kesedaran berkenaan PQC; dan

b. Mengenal pasti tahap ketersediaan inventori kriptografi terhadap risiko ancaman pengkomputeran kuantum bagi memastikan PQC dilaksanakan mengikut keutamaan.



BIDANG 07 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 - Keselamatan Kawasan

0702 - Keselamatan Peralatan

0703 - Keselamatan Persekitaran

0704 - Keselamatan Dokumen

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan

Objektif:

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

070101 Kawalan Kawasan

PERANAN: CDO dan ICTSO

Ini bertujuan untuk menghalang akses, gangguan dan kerosakan secara fizikal terhadap premis dan maklumat agensi.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;

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

c. Melindungi kawasan terhad melalui kawalan-kawalan tertentu seperti memasang alat penggera, sistem pengawasan litar tertutup, laluan keluar masuk dan kaunter kawalan;

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

e. Mereka bentuk dan melaksanakan perlindungan fizikal dan persekitaran daripada kebakaran, banjir, letupan, kacau-bilau dan bencana alam;

f. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;

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

h. Melaksanakan proses pengurusan pelawat seperti log pelawat dan polisi mengiring pelawat.

i. Menyediakan pelan kesinambungan kecemasan seperti pelaksanaan *fire drills* dan laluan evakuasi secara berkala.

070102 Kawalan Masuk Fizikal

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a. Setiap pengguna hendaklah memakai pas keselamatan sepanjang waktu bertugas;

b. Semua pas keselamatan hendaklah diserahkan kembali kepada JANM apabila berpindah keluar, berhenti atau bersara;

c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama, JANM. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan

d. Kehilangan pas mestilah dilaporkan dengan segera.

070103 Kawasan Larangan

PERANAN: Pentadbir ICT

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pengguna yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut.

Akses kepada kawasan larangan seperti pusat data dan bilik fail perlu mematuhi perkara berikut:

a. Hanya diberikan kepada pengguna yang dibenarkan sahaja; dan

b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah dipantau sepanjang masa sehingga tugas di kawasan berkenaan selesai.

0702 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT JANM daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

070201 Peralatan ICT

PERANAN: Pengguna

Peralatan ICT merangkumi peralatan komputer *desktop*, komputer riba, *server*, peralatan rangkaian dan keselamatan, media storan dan seumpamanya.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

b. Peralatan ICT yang dibekalkan adalah untuk kegunaan rasmi sahaja;

c. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO;

d. Perkakasan ICT (kecuali Komputer Riba dan *Tablet* atau peralatan yang telah mendapat kebenaran) dan fasiliti pusat data yang hendak dibawa keluar dari premis JANM perlulah mendapat kebenaran Pentadbir ICT atau Pengurus ICT dan direkodkan bagi tujuan pemantauan;

e. Panduan penggunaan komputer di JANM, hendaklah merujuk kepada Garis Panduan Penggunaan Komputer Sewaan; dan

f. Perkakasan, perisian ICT dan fasiliti pusat data yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera.

070202 Pusat Data

PERANAN: Pentadbir Pusat Data, Pentadbir Perkakasan dan Perisian

Pusat data menempatkan peralatan ICT merangkumi *server*, peralatan rangkaian dan keselamatan, peralatan storan dan seumpamanya bagi memastikan kawalan keselamatan berpusat dan dilengkapkan dengan keperluan utiliti sokongan. Pusat data diklasifikasikan sebagai kawasan larangan dan pengendalian pusat data perlu mematuhi peraturan serta garis panduan semasa yang berkuat kuasa.

070203 Media Storan

PERANAN: Pengguna

a. Data yang disimpan hendaklah di dalam media storan yang selamat. Media storan merupakan medium yang digunakan untuk menyimpan data, perisian, aplikasi dan maklumat digital seperti cakera keras, cakera padat, pita magnetik, *thumb drive* dan lain-lain;

b. Teknologi yang bersesuaian hendaklah digunakan 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; dan

c. Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Akses dan pergerakan media storan hendaklah direkodkan.

d. Penggunaan media storan ini adalah tidak digalakkan untuk menyimpan dokumen maklumat dan data rasmi yang diklasifikasikan sebagai TERHAD, SULIT, RAHSIA dan RAHSIA BESAR kecuali :

   i. Laporan Kewangan yang disimpan di PTJ sepertimana yang dinyatakan di dalam SPANM.
   ii. Penghantaran data terbuka melibatkan saiz file melebihi 5Gb.
   iii. Penyimpanan dokumen di Warchest.

   Walaubagaimanapun media storan yang digunakan tersebut hendaklah di pastikan menggunakan kaedah yang selamat seperti enkripsi, penggunaan kata laluan dan lain-lain kaedah keselamatan yang bersesuaian.

070204 Media Tandatangan Digital

PERANAN: Pengguna

Bagi menjamin keselamatan Media Sijil atau Tandatangan Digital seperti *SoftCert*, Kad Pintar, PKI *Token* dan semua pengguna perlu mengambil langkah-langkah berikut:

a. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;

b. Media ini tidak boleh dipindah milik atau dipinjamkan. Pemilik bertanggungjawab ke atas semua transaksi yang dilakukan menggunakan media tandatangan digitalnya;

c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan kepada Pegawai Yang Diberi Kuasa dan pemilik sistem dengan segera untuk tindakan seterusnya; dan

d. Pemilik sijil digital dilarang memberi pinjam, berkongsi atau bertindak sebagai *one-man-show* ketika melakukan transaksi harian yang menggunakan perakuan sijil digital. Ianya merupakan satu kesalahan di bawah Akta Tandatangan Digital 1997 [Akta 562] di bawah Seksyen 43 dan dikenakan penalti di bawah Seksyen 83.

070205 Media Perisian dan Aplikasi

PERANAN: Pentadbir ICT

Bagi menjamin keselamatan, langkah-langkah berikut hendaklah dilakukan:

a. Lesen perisian (*registration code, serials number, CD-keys*) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan

b. Hanya perisian yang berlesen dan diperakui sahaja dibenarkan bagi kegunaan JANM.

070206 Penyenggaraan Perkakasan

PERANAN: Pegawai Aset, Pentadbir ICT

Perkakasan hendaklah disenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan, kesahihan, tidak boleh disangkal dan integriti.

070207 Peralatan di Luar Premis

PERANAN: Pengguna

Perkakasan yang dibawa keluar dari premis JANM adalah terdedah kepada pelbagai risiko.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan

b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

0703 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT JANM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, kemalangan atau kecurian.

070301 Kawalan Persekitaran

PERANAN: Pengguna

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Ketua Pegawai Keselamatan Kerajaan.

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi:

a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data, (bilik percetakan, peralatan komputer, ruangan pejabat dan sebagainya) dengan teliti;

b. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;

c. Semua bahan mudah terbakar, cecair, bahan atau peralatan lain yang boleh merosakkan peralatan ICT, hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; dan

d. Semua peralatan perlindungan hendaklah dipantau dan disemak. Sebarang notifikasi atau amaran yang dikeluarkan oleh peralatan tersebut hendaklah diambil tindakan segera dan sewajarnya bagi mengelakkan sebarang insiden.

070302 Bekalan Kuasa

PERANAN: Bahagian Pembangunan Perakaunan dan Pengurusan (BPPP)

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; dan

b. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berkala atau berjadual.

070303 Kabel

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Semua kabel rangkaian komputer hendaklah diuruskan, dilindungi dan disenggara dengan kemas dan baik. Kabel rangkaian digunakan untuk menyalurkan maklumat dan boleh terdedah kepada pencerobohan.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan;

b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

d. Semua kabel di pusat data perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

070304 Prosedur Kecemasan

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan JANM 2004; dan

b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras dengan serta merta.

0704 Keselamatan Dokumen

Objektif:

Melindungi maklumat JANM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kecurian.

070401 Keselamatan Sistem Dokumentasi

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:

a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; dan

b. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.

070402 Dokumen

PERANAN: Pengguna

Bagi memastikan integriti maklumat, semua warga JANM perlu mengambil langkah-langkah berikut:

a. Penyimpanan dokumen rasmi (data terkawal dan rahsia rasmi) di storan atas talian umum adalah perlu mengikut pekeliling perkomputeran awan (*cloud computing*) dalam perkhidmatan awam yang sedang berkuatkuasa;

b. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;

c. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan;

d. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan;

e. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan

f. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.

BIDANG 08 - KESELAMATAN OPERASI

0801 - Pengurusan Prosedur Operasi

0802 - Perancangan dan Penerimaan Sistem

0803 - Perisian Berbahaya

0804 - Housekeeping

0805 - Pengelogan (*Logging*) dan Pemantauan

0806 - Kawalan Sistem Pengoperasian

0807 - Pengurusan Kerentanan Teknikal
(Technical Vulnerability Management)

BIDANG 08 KESELAMATAN OPERASI

0801 Pengurusan Prosedur Operasi

Objektif:

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

080101 Pengendalian Prosedur

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal dalam dua (2) salinan bagi tujuan rujukan dan penggunaan sekiranya berlaku bencana;

b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti untuk mencapai *Recovery Time Objective* (RTO) yang ditetapkan; dan

c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

080102 Kawalan Perubahan

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;

b. Aktiviti-aktiviti seperti memasang, menyenggara dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;

c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;

d. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal; dan

e. Perubahan luar jangka (adhoc) hendaklah memerlukan kelulusan segera dan semakan selepas pelaksanaan.

f. Proses pengurusan perubahan hendaklah dikaji semula secara berkala dan/atau apabila perubahan yang signifikan berlaku. Kajian semula hendaklah menilai:

    i. Keberkesanan proses kawalan perubahan
    ii. Pematuhan kepada dasar keselamatan dan operasi
    iii. Kecekapan mekanisme kelulusan dan pengunduran (rollback)

0802 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

080201 Perancangan Kapasiti

PERANAN: Pentadbir ICT dan ICTSO

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT pada masa akan datang.

Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

Pentadbir ICT hendaklah sentiasa memantau penggunaan sumber (resource) bagi perkara berikut:

a. Penggunaan CPU dan memori
b. Penggunaan jalur lebar rangkaian
c. Ketersediaan kapasiti storan
d. Pemantauan prestasi aplikasi

Penggunaan sumber hendaklah disemak secara berkala, dan perancangan sumber hendaklah dibangunkan bagi tujuan berikut:

a. Peningkatan sistem pada masa hadapan (pengguna baharu, penambahan bebanan kerja)
b. Penaiktarafan infrastruktur (server baharu, penambahan storan)

080202 Penerimaan Sistem

PERANAN: Pentadbir ICT dan ICTSO

Semua sistem baru (termasuklah sistem yang diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

a. Memantau pengurusan, pengagihan kapasiti, penalaan sesuatu komponen atau sistem ICT bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang;

b. Menetapkan kriteria penerimaan sistem baru, sistem yang ditingkatkan dan sistem yang diubahsuai. Pengujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem;

c. Setiap sistem yang diterima telah menjalani pengujian keselamatan yang menyeluruh dan mematuhi garis panduan pembangunan aplikasi yang sedang berkuatkuasa; dan

d. Mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti supaya dapat meminimakan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

0803 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan perisian berbahaya seperti virus, trojan dan sebagainya.

080301 Perlindungan dari Perisian Berbahaya

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memasang sistem keselamatan untuk mengesan dan mencegah perisian atau program berbahaya seperti anti-virus (perisian pengesanan), anti-spam, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS);

b. Ciri-ciri perisian pengesanan dan pencegahan perisian berbahaya hendaklah merangkumi:

   i. Pengimbasan real-time untuk perisian berbahaya dan virus.
   ii. Kemaskini automatik.
   iii. Kuarantin atau penghapusan malicious file.

c. Pengguna tidak dibenarkan untuk disable perisian pengesanan dan pencegahan perisian berbahaya pada aset mereka.

d. Memaklumkan kepada pengguna melalui program kesedaran mengenai ancaman perisian berbahaya dan kaedah menanganinya; dan

e. Setiap perisian perlu bebas daripada kelemahan, keterdedahan, virus dan aturcara tidak sah.

080302 Perlindungan Dari Mobile Code

PERANAN: Pengguna

Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

0804 Housekeeping

Objektif:

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

080401 Backup

PERANAN: Pengguna

Backup hendaklah dilakukan secara berjadual atau setiap kali konfigurasi berubah bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana atau berdasarkan keperluan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Melakukan backup ke atas semua data dan maklumat mengikut keperluan. Kekerapan backup bergantung pada tahap kritikal maklumat;

b. Backup hendaklah dilakukan di dalam media yang bersesuaian;

c. Menguji secara berkala backup dan restore bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan;

d. Menyimpan generasi backup mengikut prosedur backup dan restore; dan

e. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat mengikut prosedur yang ditetapkan.

PERANAN: Pentadbir Aplikasi

a. Memastikan salinan atau penduaan (backup) pada maklumat yang disimpan dalam perkakasan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. Maklumat yang disimpan adalah mengikut prosedur backup yang telah ditetapkan.

080402 Housekeeping Storan

PERANAN: Pentadbir Aplikasi dan Pentadbir Pangkalan Data

Housekeeping Storan mestilah dijalankan bagi memastikan ruang storan digunakan secara optimum. Aplikasi dan data yang tidak diperlukan lagi hendaklah dihapuskan dari ruang storan secara berkala.

080403 Pengorganisasian semula (Reorganisation)

PERANAN: Pentadbir Pangkalan Data

Pengorganisasian pangkalan data dan penyusunan semula ruang storan (defragmentation) mestilah dijalankan bagi memastikan pangkalan data dapat digunakan dengan optimum dengan prestasi yang terbaik.

0805 Pengelogan (Logging) dan Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

080501 Pemantauan

PERANAN: Pentadbir ICT

Perkara-perkara berikut perlu dipatuhi untuk memantau aktiviti yang tidak dibenarkan:

a. Sebarang percubaan pencerobohan dan ancaman kepada sistem ICT seperti kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery), penyamaran (phishing), pencerobohan (intrusion), ancaman (threats) dan kehilangan data (data loss);

b. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sistem tanpa kebenaran;

c. Aktiviti-aktiviti yang tidak produktif seperti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;

d. Aktiviti pewujudan perkhidmatan yang tidak dibenarkan; dan

e. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian.

080502 Jejak Audit

PERANAN: Pentadbir ICT

Setiap sistem mestilah mempunyai jejak audit (audit trail). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem mengikut kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan.

Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

a. Rekod setiap aktiviti transaksi;

b. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;

c. Aktiviti capaian pengguna ke atas sistem sama ada secara sah atau sebaliknya; dan

d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Menyimpan jejak audit untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara;

b. Menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan membantu mengesan aktiviti yang tidak normal dengan lebih awal;

c. Melindungi jejak audit daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan; dan

d. Menyenggara jejak audit dari semasa ke semasa.

080503 Sistem Log

PERANAN: Pentadbir ICT

Sistem log diwujudkan untuk merekod semua aktiviti harian pengguna bagi sistem kritikal.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memastikan fail log bagi server dan aplikasi di JANM diaktifkan:

   i. Fail log sistem pengoperasian;
   ii. Fail log servis (laman web, File Transfer Protocol (FTP), e-mel);
   iii. Fail log aplikasi (audit trail);
   iv. Fail log rangkaian (switch, firewall, router, IDS/IPS); dan
   v. Fail log backup.

b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;

c. Menyimpan fail log untuk tempoh sekurang-kurangnya enam (6) bulan di tempat selamat dan dikemukakan kepada NACSA apabila diperlukan untuk pengendalian insiden keselamatan ICT;

d. Melaporkan kepada ICTSO dan CDO sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan; dan

e. Menyenggara sistem log dari semasa ke semasa.

080504 Perlindungan Maklumat Log

PERANAN: Pentadbir ICT

Perkara-perkara yang mesti dipatuhi adalah seperti berikut :-

a. Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap;

b. Memantau penggunaan kemudahan memproses maklumat secara berkala;

c. Kesalahan, kesilapan atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan

e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada pasukan CSIRT JANM.

080505 Log Pentadbir dan Pengendali

PERANAN: Pentadbir ICT

Perkara-perkara yang mesti dipatuhi adalah seperti berikut :-

a. Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap;

b. Memantau penggunaan kemudahan memproses maklumat secara berkala;

c. Kesalahan, kesilapan atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan

e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada pasukan CSIRT JANM.

080506 Penyelarasan Waktu

PERANAN: Pentadbir ICT

Memastikan penyelarasan waktu dengan satu sumber waktu yang sah (Network Time Protocol - NTP) bagi sistem pemprosesan maklumat dan domain keselamatan.

0806 Kawalan Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

PERANAN: Pentadbir Perkakasan dan Perisian

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti berikut:

a. Strategi "backup" perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;

b. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian diperakui berjaya; dan

c. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

0807 Pengurusan Kerentanan Teknikal (Technical Vulnerability Management)

Objektif:

Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

080701 Pengurusan Kerentanan ICT

PERANAN: ICTSO dan Pentadbir ICT

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperolehi dari sumber yang betul. Mekanisma eksplotasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan.

Kawalan keselamatan atau security patches hendaklah dikemas kini ke atas perkakasan, aplikasi dan sistem operasi yang digunakan.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Melaksanakan ujian penembusan untuk memperolehi maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

b. Menganalisis tahap risiko kerentanan;

c. Mengambil tindakan pengolahan dan kawalan risiko; dan

d. Keperluan dan aktiviti audit kerentanan (seperti Security Posture Assessment) yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas perkhidmatan JANM.

080702 Sekatan ke atas Pemasangan Perisian

PERANAN: Pengguna

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut:

a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pengguna.

b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; dan

c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;

d. Sebarang instalasi perisian tambahan hendaklah mendapat kebenaran Pentadbir ICT.

0808 Pencegahan Ketirisan Data

Objektif:

Memastikan langkah-langkah pencegahan kebocoran data dilaksanakan pada sistem, rangkaian dan sebarang peranti lain yang memproses, menyimpan atau menghantar maklumat terperingkat.

080801 Pelaksanaan Pencegahan Ketirisan Data

PERANAN: Warga JANM, Pengguna

Data dan maklumat didalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Tindakan yang perlu dilaksanakan ialah seperti berikut:

a. Mengenal pasti dan mengelaskan data dan maklumat untuk dilindungi daripada ketirisan;

b. Memantau saluran transaksi dan perkongsian data dan maklumat terperingkat (contoh penggunaan SPDT, e-mel, pemindahan fail, perkhidmatan peranti atau media mudah alih); dan

c. Melaksanakan pengukuhan (contoh: hardening, patching) untuk mengelakkan ketirisan maklumat.

0809 Pengurusan Konfigurasi

Objektif:

Memastikan konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian ICT berfungsi dengan baik dan mengambil kira aspek keselamatan.

080901 Pengurusan Penetapan Konfigurasi

PERANAN: ICTSO, Pentadbir

Mewujudkan dan mengemaskini pengurusan konfigurasi sebagai garis dasar (baseline) untuk teknologi yang digunakan melibatkan kategori aset berikut sebelum ia ditempatkan (deployed):

a. Perkakasan (Hardware)

b. Perisian (Software)

c. Perkhidmatan (Services)

d. Rangkaian (Networks)

Sekiranya proses konfigurasi tidak tersedia untuk teknologi tertentu, jabatan berkaitan hendaklah menyelidik dan menentukan konfigurasi keselamatan yang sesuai sebelum menempatkan produk tersebut.

Teknologi dengan secure configuration hendaklah dipantau secara berterusan dan dikaji semula untuk memastikan pematuhan berterusan dengan tetapan yang diluluskan.

BIDANG 09 - KESELAMATAN KOMUNIKASI

0901 - Pengurusan Rangkaian

0902 - Pengurusan Pertukaran Maklumat

0903 - Perkhidmatan Atas Talian/eDagang dan Maklumat Umum

BIDANG 09 KESELAMATAN KOMUNIKASI

0901 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

090101 Kawalan Infrastruktur Rangkaian

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Mengawal capaian peralatan rangkaian kepada pengguna yang dibenarkan sahaja;

b. Memasang peranti keselamatan yang dapat mengawal aliran trafik dan menghalang sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JANM;

c. Mengawal penyambungan kepada sistem rangkaian; dan

d. Melaksanakan segmen rangkaian yang berasingan bagi peranti pengkomputeran peribadi milik persendirian untuk capaian *internet* bagi urusan tidak rasmi melalui *wifi* JANM-*Guest*.

090102 Perkhidmatan Keselamatan Rangkaian

PERANAN: ICTSO dan Pentadbir Rangkaian dan Keselamatan ICT

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pihak ketiga;

b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit; dan

Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

090103 Pengasingan Perkakasan dan Rangkaian

PERANAN: Pentadbir Rangkaian dan Keselamatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Perkakasan berkaitan yang digunakan bagi tugas membangun, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*;

b. Pengasingan juga merangkumi tindakan memisahkan rangkaian antara kumpulan operasi *(production)* dan pembangunan atau pengujian *(development or testing);* dan

c. Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JANM.

0902 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara JANM dan agensi luar terjamin. Pertukaran maklumat meliputi perkongsian data terbuka bertujuan untuk peningkatan kualiti dan ketelusan penyampaian perkhidmatan kerajaan serta menggalakkan pertumbuhan ekonomi negara.

090201 Pertukaran Maklumat

PERANAN: Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

b. Pertukaran maklumat dan perisian di antara JANM dengan agensi luar perlu dibuat secara rasmi atau mewujudkan perjanjian jika perlu;

c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JANM;

d. Pemindahan maklumat secara elektronik hendaklah dilindungi bagi memastikan ianya selamat; dan

e. Melaksanakan penyamaran data dengan melaksanakan proses penyembunyian data sebenar yang melibatkan PII.

090202 Perjanjian Pemindahan Data dan Maklumat

PERANAN: Pengurus ICT dan Pentadbir ICT

Pengurus ICT hendaklah mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara JANM dengan pihak luar.

Perkara yang perlu dipertimbangkan adalah:

a. Pengurus ICT hendaklah mengawal penghantaran dan penerimaan maklumat JANM;

b. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat JANM;

c. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

d. Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

090203 Pengurusan Mel Elektronik (E-mel)

PERANAN: Pentadbir E-mel

Penggunaan e-mel di JANM hendaklah dipantau secara berterusan untuk memenuhi keperluan etika penggunaan e-mel dan Internet serta mana-mana undang-undang bertulis yang berkuat kuasa.

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

a. Pemilikan akaun e-mel rasmi JANM adalah dengan kelulusan penyelia;

b. Melakukan pembersihan kandungan (*content sanitization*) pada rantaian e-mel mengikut prinsip perlu mengetahui (*need to know basis*);

c. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan atau tidak diperlukan lagi boleh dihapuskan;

d. Menamatkan akaun dengan segera jika melanggar dasar atau tatacara JANM atas tujuan keselamatan maklumat dengan menggunakan Borang Penamatan Perkhidmatan MyGovUC dan *Active Directory*; dan

e. Akaun e-mel perlu ditamatkan sebaik sahaja menerima *Request to Delete* (RTD) bergantung pada tarikh pengguna tamat perkhidmatan di JANM atau bertukar Kementerian atau Jabatan.

0903 Perkhidmatan Atas Talian/eDagang dan Maklumat Umum

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan atas talian daripada sebarang risiko seperti penyalahgunaan, kecurian dan pindaan maklumat yang tidak sah dapat dihalang.

090301 Perkhidmatan Atas Talian dan eDagang

PERANAN: Pengguna

Menggalakkan pertumbuhan perkhidmatan atas talian sebagai menyokong hasrat kerajaan mempelbagaikan saluran sistem penyampaian perkhidmatan awam melalui aplikasi e-Kerajaan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengenalan pengguna kepada orang awam digunakan untuk aplikasi e-Kerajaan dalam penyampaian perkhidmatan awam;

b. Maklumat yang disimpan di dalam perkhidmatan atas talian perlu dilindungi daripada aktiviti penipuan, pendedahan dan pengubahsuaian yang tidak dibenarkan;

c. Maklumat transaksi atas talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi dan duplikasi; dan

d. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

090302 Maklumat Umum

PERANAN: Pengguna

Maklumat umum merupakan hebahan maklumat yang boleh dicapai oleh orang awam melalui perkhidmatan elektronik.

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut:

a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;

b. Memastikan segala maklumat telah disah dan diluluskan sebelum dipaparkan; dan

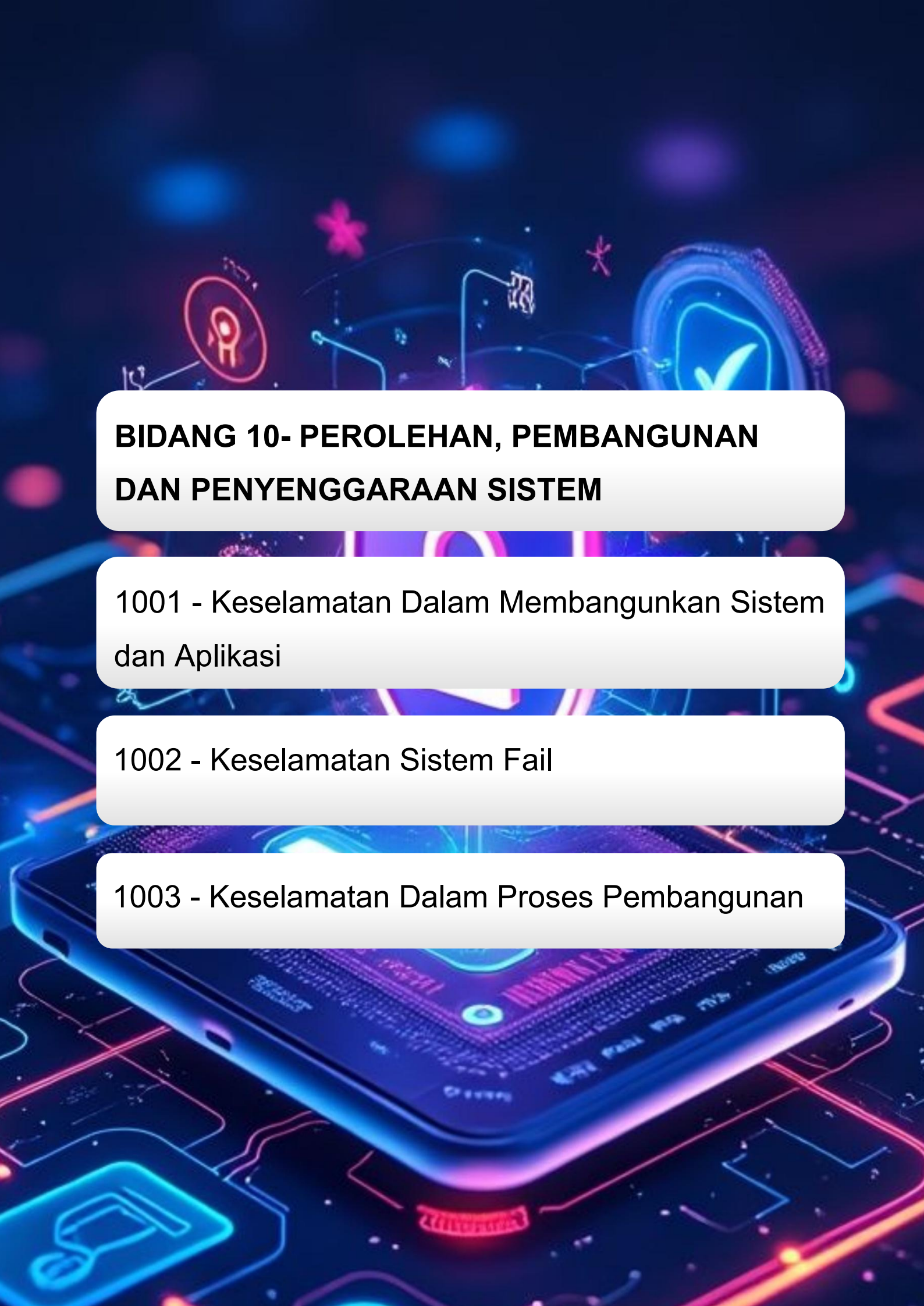
c. Melakukan pengemaskinian dan penyenggaraan agar sentiasa memaparkan maklumat terkini.

090303 Perjanjian Kerahsiaan Atau Ketakdedahan

PERANAN: Pengurus ICT

Syarat-syarat perjanjian kerahsiaan (*Non-disclosure agreement)* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan.

Pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.



BIDANG 10- PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

1001 - Keselamatan Dalam Membangunkan Sistem dan Aplikasi

1002 - Keselamatan Sistem Fail

1003 - Keselamatan Dalam Proses Pembangunan

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

100101 Keperluan Keselamatan Sistem Maklumat

PERANAN: Pemilik Sistem, Pentadbir ICT dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Perolehan, pembangunan, penambahbaikan dan penyenggaraan sistem hendaklah diberikan keutamaan kepada produk, kepakaran dan teknologi tempatan;

b. Perolehan, pembangunan, penambahbaikan dan penyenggaraan sistem hendaklah menerapkan prinsip *zero trust*, di mana akses hanya diberikan kepada pengguna yang dibenarkan melalui mekanisme kawalan keselamatan yang berterusan;

c. Aplikasi baharu yang dibangunkan perlu mematuhi panduan pengekodan yang selamat *(secure coding)*;

d. Perolehan, pembangunan, penambahbaikan dan penyenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tiada sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;

e. Spesifikasi perolehan hendaklah memasukkan keperluan pensijilan minima keselamatan maklumat bagi pasukan projek;

f. Pemilihan syarikat pembekal hendaklah mengikut peraturan semasa yang sedang berkuatkuasa dan berdasarkan rangka kerja keselamatan siber;

g. Keselamatan sistem maklumat bagi aplikasi baharu harus dipastikan melalui pengujian dalam fasa pembangunan untuk mematuhi keperluan keselamatan JANM;

h. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan dalam sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna;

i. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan ketidak sahihan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan;

j. Sistem yang dibangunkan hendaklah dibuat *Security Posture Assessment* (SPA) atau penilaian tahap risiko bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan;

k. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dibuat SPA atau penilaian tahap risiko bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; dan

l. Pensijilan keselamatan ke atas sistem bagi pematuhan kepada standard keselamatan ICT bagi memastikan keteguhan kawalan keselamatan ICT dan boleh beroperasi antara satu sama lain hendaklah diperolehi daripada agensi pensijilan yang diiktiraf oleh kerajaan.

100102 Penerimaan Sistem dan Aplikasi

PERANAN: Pentadbir Perkakasan dan Perisian dan ICTSO

Semua sistem atau aplikasi baharu (termasuklah sistem atau aplikasi yang diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

a. Memantau pengurusan, pengagihan kapasiti, penalaan sesuatu komponen atau sistem ICT bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang;

b. Menetapkan kriteria penerimaan sistem baru, sistem yang ditingkatkan dan sistem yang diubahsuai. Pengujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem;

c. Penerimaan sistem dan aplikasi bergantung kepada penerimaan semua fasa pengujian keselamatan sistem;

d. Mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti supaya dapat meminimakan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang;

e. Memastikan perkakasan dan perisian ICT yang memenuhi keperluan sistem atau aplikasi serta operasi perkhidmatan dilaksanakan dengan cekap dan berkesan;

f. Pengagihan perkakasan dan perisian ICT hendaklah mengikut keperluan kerja dan kapasiti semasa dengan perakuan dan mendapat kelulusan daripada Pengurus ICT/ICTSO; dan

g. Prosedur penerimaan sistem dan aplikasi perlu mematuhi prinsip *zero trust,* di mana akses hanya diberikan kepada pengguna yang dibenarkan melalui mekanisme kawalan keselamatan yang berterusan. Ini melibatkan penilaian keselamatan terhadap verifikasi identiti, penyulitan dan pengasingan tugas dan tanggungjawab *(segregation of duties)*.

100103 Pengesahan Data Input dan Output

PERANAN: Pemilik Sistem dan Pentadbir Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan

b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

100104 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam

PERANAN: Pentadbir Aplikasi

Perkara yang perlu dipertimbangkan adalah seperti berikut:

a. 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 JANM. Contoh perkhidmatan sumber luaran ialah:

   i. Perisian Sebagai Satu Perkhidmatan;
   ii. Platform Sebagai Satu Perkhidmatan;
   iii. Infrastruktur Sebagai Satu Perkhidmatan;
   iv. Storan Pengkomputeran Awan; dan
   v. Pemantauan Keselamatan;

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

c. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*);

d. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

e. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

f. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

1002 Keselamatan Sistem Fail

Objektif:

Memastikan supaya sistem fail dikawal dan dikendalikan dengan baik dan selamat.

100201 Kawalan Sistem Fail

PERANAN: Pemilik Sistem dan Pentadbir Perkakasan dan Perisian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Proses pengemaskinian sistem fail hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;

b. Sebarang pindaan ke atas kod sumber aturcara *(program source code)* hanya boleh dilaksanakan atau digunakan selepas pengujian;

c. Mengawal capaian ke atas kod sumber aturcara bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;

d. Memilih data yang sesuai untuk ujian;

e. Kawalan keselamatan perlu dilakukan ke atas fail dan data ujian sebelum pengujian dilakukan; dan

f. Mengaktifkan audit *log* bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

1003 Keselamatan Dalam Proses Pembangunan dan Sokongan Aplikasi

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

100301 Prosedur Kawalan Perubahan

PERANAN: Pemilik Sistem dan Pentadbir Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;

b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga;

c. Perubahan dan/atau pindaan ke atas pakej perisian perlu dikawal dan dihadkan mengikut keperluan;

d. Akses kepada kod sumber aturcara perlu dihadkan kepada pengguna yang dibenarkan; dan

e. Sebarang peluang untuk membocorkan maklumat perlu dihalang.

100302 Pembangunan Aplikasi dan Perisian Secara *Outsource*

PERANAN: Pemilik Sistem dan Pentadbir Aplikasi

Pembangunan aplikasi dan perisian oleh pihak ketiga perlu dikawal selia, dipantau dan disemak.

Memastikan sistem ICT yang disediakan kepada Warga JANM sentiasa dalam keadaan selamat dan dilindungi dengan mengambil kira keselamatan data-dalam-simpanan (*data-at-rest*), data-dalam-pergerakan (*data-in-motion*) dan data-dalam-penggunaan (*data-in-use*).

Kod sumber aturcara bagi semua aplikasi dan perisian yang dibangunkan menjadi hak milik JANM.

Bagi pembangunan secara *outsource*, pembekal yang dilantik berkebolehan untuk mengenalpasti dan menambahbaik kelemahan dalam pembangunan sistem/aplikasi.

100303 Pengujian Keselamatan Sistem

PERANAN: Pentadbir Aplikasi

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan aplikasi.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;

b. Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti kesilapan maklumat; dan

c. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.

Memastikan pengujian keselamatan ke atas perisian dan aplikasi sistem dijalankan semasa pembangunan diikuti dengan pengujian penembusan (*penetration testing*) sebelum penempatan (*deployment*) dalam persekitaran *production* dan *public facing*. Pengujian keselamatan pra-penempatan hendaklah merangkumi:

a. Imbasan kelemahan (*Vulnerability scans*) untuk mengesan kelemahan;

b. Pengujian penembusan (*Penetration testing*) untuk mensimulasikan senario serangan;

c. Pematuhan kepada panduan pengekodan selamat (*secure coding*) bagi pembangunan sistem yang baharu; dan

d. Lain-lain pematuhan yang berkaitan dan diperlukan.

100304 Pengujian Penerimaan Sistem

PERANAN: Pemilik Sistem dan Pentadbir Aplikasi

Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk **100101** dan **100102**);

b. penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan

c. pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanning).*

100305 Data Ujian

PERANAN: Pemilik Sistem dan Pentadbir Aplikasi

Data ujian hendaklah dilindungi dan dikawal.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; dan

b. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian.

Perkara yang perlu dipertimbangkan adalah seperti berikut:

a. Mengaktifkan audit *log* bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.

BIDANG 11- HUBUNGAN PEMBEKAL

1101 - Pihak Ketiga

BIDANG 11 HUBUNGAN PEMBEKAL

1101 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT JANM yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

110101 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal

PERANAN: CDO, ICTSO, Pengurus ICT, Pentadbir ICT dan Pihak ketiga

Ini bertujuan memastikan penggunaan maklumat dan kemudahan pemprosesan maklumat oleh pihak ketiga dikawal sama ada untuk pelaksanaan projek ICT atau tindakan *outsource* perkhidmatan tertentu.

Perkara yang perlu dipatuhi oleh Pengurus ICT termasuk yang berikut:

a. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; dan
b. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JANM.

Perkara yang perlu dipatuhi oleh Pihak ketiga termasuk yang berikut:

a. Membaca, memahami dan mematuhi PKS JANM;
b. Melakukan capaian ke atas aset ICT JANM berdasarkan kepada perjanjian kontrak;
c. Menandatangani Surat Akuan Pematuhan PKS JANM sebagaimana **Lampiran 2**; dan
d. Mematuhi arahan keselamatan yang berkuatkuasa.

Perkara yang perlu dipatuhi oleh Pentadbir ICT JANM berhubung keperluan keselamatan maklumat dengan pihak ketiga termasuk yang berikut:

a. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran akses kepada pihak ketiga; dan

b. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran akses atau penggunaan kepada pihak ketiga.

110102 Keperluan Keselamatan Dalam Perjanjian Pembekal

PERANAN: Pihak Ketiga dan Pengurus ICT

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi.

Syarikat pembekal hendaklah memastikan semua personel mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam menjalankan perkhidmatan kepada pihak JANM selaras dengan peraturan dan kawalan keselamatan yang berkuatkuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. JANM hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan (MOF) dalam Kod Bidang yang berkaitan;

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

c. Wakil atau personel syarikat pembekal hendaklah mempunyai pensijilan keselamatan (*security certification*) yang berkaitan;

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

e. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak berdasarkan prestasi syarikat pembekal; dan

f. Prestasi pembekal hendaklah dipantau, disemak dan dinilai.

110103 Pengenalpastian dan Pendokumentasian Pembekal Perkhidmatan Luaran

PERANAN: Pihak Ketiga dan Pengurus ICT

Semua pembekal perkhidmatan luaran yang mengendalikan infrastruktur ICT, perisian atau data dan maklumat terperingkat hendaklah dikenal pasti, didokumenkan dan dikemaskini seperti berikut:

a. **Maklumat Pembekal** – Nama, butiran dan peranan pembekal perkhidmatan.

b. **Skop Perkhidmatan** – Huraian mengenai perkhidmatan yang disediakan.

c. **Pengendalian Data** – Butiran mengenai sebarang data/maklumat terperingkat yang diakses atau diproses.

d. **Tahap Risiko** – Penilaian terhadap risiko keselamatan siber dan risiko operasi yang berkaitan dengan pembekal

e. **Status Pematuhan** – Pematuhan pembekal terhadap piawaian keselamatan yang berkaitan (contohnya, ISO/IEC 27001) dan pematuhan kontraktual. Pematuhan ini boleh merangkumi saringan latar belakang terhadap kakitangan yang terlibat dengan perkhidmatan, bergantung pada penilaian risiko organisasi.

f. **Butiran Kontrak** – Rujukan kepada sebarang perjanjian atau kontrak yang ada, termasuk klausa yang berkaitan dengan perlindungan data, keperluan keselamatan, dan pemberitahuan pelanggaran.

BIDANG 12- PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

1201- Penilaian Risiko Keselamatan ICT

1202- Rawatan Risiko Keselamatan ICT

BIDANG 12 PENGURUSAN RISIKO KESELAMATAN ICT

1201 Penilaian Risiko Keselamatan ICT

Objektif:

Memastikan penilaian risiko dilaksanakan dengan berkesan bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

120101 Tanggungjawab dan Prosedur

PERANAN: Pengurus ICT, dan Pemilik Sistem

Mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

Mengenal pasti organisasi keselamatan ICT dan struktur tadbir urus pengurusan risiko untuk:

a. mengenal pasti kerentanan;

b. mengenal pasti ancaman;

c. menilai risiko;

d. menentukan pengolahan risiko;

e. memantau keberkesanan pengolahan risiko; dan

f. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

Item **(e)** dan **(f)** di atas hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun dalam mesyuarat jawatankuasa berkaitan.

Melaksanakan penilaian risiko keselamatan ICT sekurang-kurangnya sekali setahun atau terdapatnya perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengelak, mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko ICT.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat termasuklah aplikasi, perisian, *server*, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Pelaksanaan dan pengurusan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan berlakunya risiko dengan memilih tindakan berikut:

a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b. menerima atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan JANM;

c. mengelak atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

1202 Rawatan Risiko Keselamatan ICT

Objektif:

Memastikan pendekatan yang efektif digunakan bagi tahap segera rawatan yang diperlukan mengikut penilaian risiko yang telah dilaksanakan.

120201 Rangka Kerja

PERANAN: Pentadbir ICT dan Pemilik Sistem

Merangka Pelan Rawatan Risiko (RTP) yang menggariskan tindakan mengikut keutamaan berdasarkan tahap risiko serta tahap segera rawatan yang diperlukan.

Bagi setiap risiko yang dikenal pasti dalam RTP, maklumat pelaksanaan terperinci hendaklah dipantau dan didokumenkan. Maklumat ini hendaklah merangkumi, tetapi tidak terhad kepada:

a. **Pilihan rawatan risiko** – Pilihan boleh termasuk pengekalan risiko, pengubahsuaian risiko, perkongsian risiko dan pengelakan risiko.

b. **Kawalan rawatan risiko** – Langkah atau tindakan khusus untuk mengurangkan risiko.

c. **Pelantikan pemilik risiko** – Individu atau pasukan yang bertanggungjawab ke atas pengurusan risiko.

d. **Pelantikan individu bertanggungjawab ke atas pelaksanaan** – Individu atau pasukan yang ditugaskan untuk melaksanakan aktiviti rawatan.

e. **Risiko baki (*residual risk*)** – Tahap risiko yang masih kekal selepas pelaksanaan kawalan rawatan.

RTP hendaklah disemak dan diluluskan oleh jawatankuasa tadbir urus keselamatan siber yang berkaitan, Bagi meluluskan pelan tersebut, pemilik risiko hendaklah menilai kawalan yang dicadangkan dalam RTP untuk menilai keberkesanannya dalam mengurangkan kemungkinan dan/atau impak risiko yang dikenal pasti.

RTP yang telah diluluskan hendaklah dilaksanakan dan keberkesanan pelaksanaannya perlu dipantau serta disemak secara berterusan dalam mesyuarat jawatankuasa tadbir urus keselamatan siber yang ditubuhkan.

Kemajuan pelaksanaan pelan hendaklah dilaporkan secara berkala dengan status yang jelas, dikategorikan seperti berikut:

a. **Belum Bermula (*Not Started*)** – Tugas atau kawalan yang belum dimulakan.

b. **Sedang Dilaksanakan (*In Progress*)** – Tugas atau kawalan yang sedang dilaksanakan.

c. **Selesai (*Completed*)** – Tugas atau kawalan yang telah dilaksanakan sepenuhnya.

Hasil daripada rawatan risiko hendaklah didokumenkan dan dilaporkan kepada tadbir urus atau JKICT yang berkaitan.

BIDANG 13 - PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

1301 - Mekanisme Pelaporan Insiden Keselamatan ICT

1302 - Pengurusan Maklumat Insiden Keselamatan ICT

BIDANG 13 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

1301 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

130101 Tanggungjawab dan Prosedur

PERANAN: Pengurus ICT, CSIRT JANM dan Pemilik Sistem

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.

Pengurusan insiden JANM adalah berdasarkan kepada Prosedur Pengurusan Pengendalian Insiden yang sedang berkuatkuasa.

Perkara yang perlu dipatuhi adalah seperti berikut:

a. Memberi kesedaran berkaitan Prosedur Pengendalian Insiden dan hebahan kepada warga JANM sekiranya ada perubahan; dan

b. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

130102 Pelaporan Kejadian Keselamatan Maklumat

PERANAN: Pengguna dan CSIRT JANM

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin mengikut proses di **Lampiran 3.**

Tanggungjawab CSIRT JANM termasuklah:

a. Mengesan atau menerima aduan insiden keselamatan ICT dan menilai tahap serta jenis insiden;

b. Merekod dan menjalankan siasatan awal insiden yang diterima;

c. Melaporkan insiden kepada ICTSO atau Pengurus CSIRT JANM;

d. Menangani insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

e. Mengesyorkan kepada CDO atau Pengarah CSIRT mengambil tindakan pemulihan dan pengukuhan; dan

f. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada JANM.

Perkara yang perlu dipertimbangkan adalah seperti berikut:

a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;

b. Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;

c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;

e. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan;

f. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

g. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan ICT mesti mematuhi:

a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan

b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

1302 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

130201 Tindak Balas Terhadap Insiden Keselamatan Maklumat

PERANAN: Pentadbir ICT dan CSIRT JANM

Insiden keselamatan maklumat hendaklah diuruskan menurut prosedur yang didokumenkan.

130202 Pengumpulan Bahan Bukti

PERANAN: ICTSO dan Pentadbir ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang.

Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada JANM. Carta Alir Pelaporan Insiden Keselamatan ICT adalah seperti di **Lampiran 3**.

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut:

a. Menyimpan jejak audit, *backup* secara berkala dan melindungi semua bahan bukti bagi menjamin integriti;

b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

c. Menyediakan pelan kontingensi dan pelan kesinambungan perkhidmatan;

d. Menyediakan pelan tindakan pemulihan segera; dan

e. Memaklum atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

130203 Forensik ICT

PERANAN: Pentadbir ICT dan CSIRT JANM

Langkah-langkah yang perlu diambil untuk forensik ICT adalah seperti berikut:-

a. Mengumpulkan bahan bukti seperti *log*, *hard disk* atau media storan yang berkenaan;

b. Melakukan siasatan awal;

c. Mendapatkan kepakaran untuk menganalisis bahan bukti;

d. Memastikan bahan-bahan bukti sentiasa dipantau mengikut rantaian jagaan (*chain of custody*) yang rapi agar kesahihan bukti tidak terjejas;

e. Melaksanakan tindakan baik pulih dan pengukuhan; dan

f. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan.

BIDANG 14 - ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1401 - Kesinambungan Perkhidmatan

BIDANG 14 ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1401 Kesinambungan Perkhidmatan

Objektif:

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

140101 Pelan Kesinambungan Perkhidmatan

PERANAN: Sekretariat PKP JANM dan Koordinator Bahagian / Pejabat Perakaunan

Jawatankuasa dan Pasukan (*team*) yang sesuai untuk mengkaji dan merancang Pelan Kesinambungan Perkhidmatan hendaklah ditubuhkan. Keahlian dan jawatankuasa yang terlibat hendaklah terdiri dari mereka yang berpengalaman dan memahami konteks perkhidmatan dan keperluan kesinambungan perkhidmatan JANM.

Pelan Kesinambungan Perkhidmatan (*Business Continuity Management* - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Pelan ini perlu diperakui dan dipantau oleh pengurusan JANM.

Perkara-perkara berikut perlu dipatuhi dan diberi perhatian:

a. Mengenal pasti dan mendokumenkan semua tanggungjawab, prosedur dan proses kecemasan atau pemulihan yang dipersetujui;

b. Mengenal pasti insiden yang boleh mengakibatkan gangguan terhadap proses bisnes dan impak gangguan tersebut kepada penyampaian perkhidmatan JANM;

c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam masa yang ditetapkan;

d. Menyimpan salinan pelan BCM di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama;

e. Menguji (simulasi) dan mengemaskini Pelan BCM secara berjadual bagi memastikan keberkesanannya dengan merujuk kepada:

   i. Polisi BCM*;*
   ii. Laporan *Business Impact Analysis*;
   iii. *Business Recovery Strategy*;
   iv. *IT Recovery Strategy*;
   v. *Incident Management Plan*;
   vi. *Business Continuity Plan*; dan
   vii. *Acitivity Response Plan*.

f. Memastikan warga JANM perlu mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

Pelan Kesinambungan Perkhidmatan mengandungi perkara-perkara berikut:

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

b. Senarai personel JANM dan vendor berserta nombor yang boleh dihubungi (telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel (*alternate*) yang tidak dapat hadir untuk menangani insiden;

c. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

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

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

BIDANG 15 - PEMATUHAN

1501 - Pematuhan dan Keperluan Perundangan

BIDANG 15 PEMATUHAN

1501 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada PKS JANM.

150101 Pematuhan Dasar

PERANAN: Pengguna

Setiap pengguna ICT JANM hendaklah membaca, memahami dan mematuhi PKS JANM dan undang-undang atau peraturan-peraturan berkaitan yang berkuat kuasa.

Semua aset ICT di JANM termasuk maklumat yang disimpan di dalamnya ialah hak milik Kerajaan. ANM dan pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT JANM selain daripada maksud dan tujuan yang telah ditetapkan, merupakan satu penyalahgunaan sumber JANM.

150102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

PERANAN: ICTSO

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.

Pengauditan terhadap pematuhan PKS hendaklah dijalankan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.

150103 Pematuhan Keperluan Audit

PERANAN: Warga JANM

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan sistem audit maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

150104 Keperluan Perundangan

PERANAN: Pengguna

Senarai Perundangan Dan Peraturan yang perlu dipatuhi oleh semua pengguna ICT JANM adalah seperti di **Lampiran 4**.

150105 Pelanggaran Dasar

PERANAN: Pengguna

Pelanggaran PKS JANM boleh dikenakan tindakan tatatertib oleh Ketua Perkhidmatan mengikut Perintah Am Bab D. Kesalahan jenayah hendaklah dikuatkuasakan oleh Polis Diraja Malaysia (PDRM).

GLOSARI

PERKATAAN	DEFINISI
ANM	Akauntan Negara Malaysia
BPPP	Bahagian Pembangunan Perakaunan dan Pengurusan
BPTM	Bahagian Pengurusan Teknologi Maklumat
BYOD	Peranti Pengkomputeran Peribadi atau *Bring Your Own Devices*
CERT	*Computer Emergency Response Team atau Pasukan Tindak Balas Kecemasan Komputer*
CSIRT	*Cyber Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT
CDO (*Chief Digital Officer)*	Ketua Pegawai Digital, iaitu pegawai yang dilantik untuk menjadi peneraju inisiatif pendigitalan di kementerian melalui penggunaan data, analitis dan teknologi digital.
CGSO (*Chief Government Security Office*)	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia.
Data Masking	Suatu teknik penyamaran data yang sensitif, di mana ianya memastikan data kekal selamat ketika pembangunan, pengujian atau senario lain yang berkaitan.
FTP	*File Transfer Protocol*

PERKATAAN	DEFINISI
GPKI	*Government Public Key Infrastructure*
GPTMK	Garis Panduan Teknologi Maklumat dan Komunikasi
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* atau Pegawai Keselamatan ICT
IDS	*Intrusion Detection System*
IoT	*Internet of Things*
IPS	*Intrusion Prevention System*
IPN	Institut Perakaunan Negara
ISP	Pelan Stategik ICT (ISP)
JANM	Jabatan Akauntan Negara Malaysia
JDN	Jabatan Digital Negara
JKICT	Jawatankuasa Keselamatan ICT
JKKICT	Jawatankuasa Kerja Keselamatan ICT
JPICT	Jawatankuasa Pemandu ICT

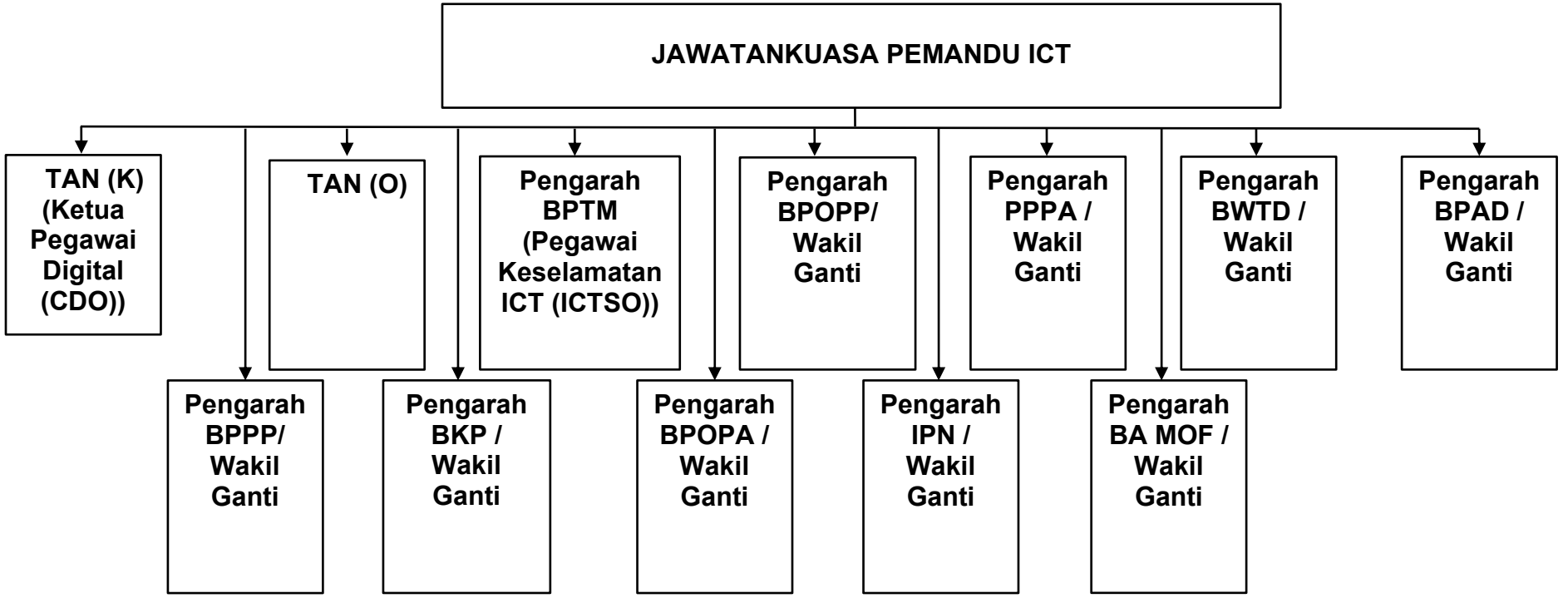
PERKATAAN	DEFINISI
LAN	*Local Area Network*
MFA	Multi-Factor Authentication
MOF	Kementerian Kewangan (MOF)
NACSA	*National Cyber Security Agency*
NTP	*Network Time Protocol*
PDRM	Polis Diraja Malaysia
PDA	*Personal Digital Assistances* atau Pembantu Digital Peribadi
PKJ	Pegawai Keselamatan Jabatan
PKI	*Public-Key Infrastructure* atau Prasarana Kunci Awam
PKP	Pengurusan Kesinambungan Perkhidmatan *atau Business Continuity Management*
PKS	Polisi Keselamatan Siber
PII	*Personally Identifiable Information* atau Maklumat Pengenalan Peribadi
PQC	Kriptografi Pasca Kuantum atau *Post-Quantum Cryptography*
PSP	Pelan Strategik Pendigitalan

PERKATAAN	DEFINISI
PTK	Penilaian Tahap Keselamatan
RTD	*Request to Delete*
RTO	*Recovery Time Objective*
SPA	*Security Posture Assestment*
SPDT	Sistem Penghantaran Dokumen Sulit dan Terhad
SPANM	Surat Pekeliling Akauntan Negara Malaysia
SSL	*Secure Socket Layer*
USB	*Universal Serial Bus*
URK	Unit Pengurusan Rangkaian dan Keselamatan ICT.
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
Zero Trust	*Zero Trust* bermakna akses kepada sumber aset ICT tidak diberikan kepada pengguna secara automatik. Pengesahan diperlukan daripada pentadbir untuk mendapatkan akses bagi mengelakkan pelanggaran data.

Lampiran 1

STRUKTUR ORGANISASI

JAWATANKUASA PEMANDU ICT JANM



Lampiran 2

AKUAN PEMATUHAN POLISI KESELAMATAN SIBER (PKS)

JABATAN AKAUNTAN NEGARA MALAYSIA (JANM)

Nama	:	
No. Kad Pengenalan	:	
Jawatan	:	
Kementerian/Jabatan/Organisasi	:	

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber JANM;
2. Saya mengaku membawa **peranti perkomputeran peribadi yang disahkan selamat ke JANM dan mencapai maklumat rasmi menggunakan peranti tersebut; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

(Tandatangan Pegawai)

Tarikh : .....

Pengesahan

.....

(Tandatangan Pegawai Pengesah)

Nama Pegawai Pengesah :

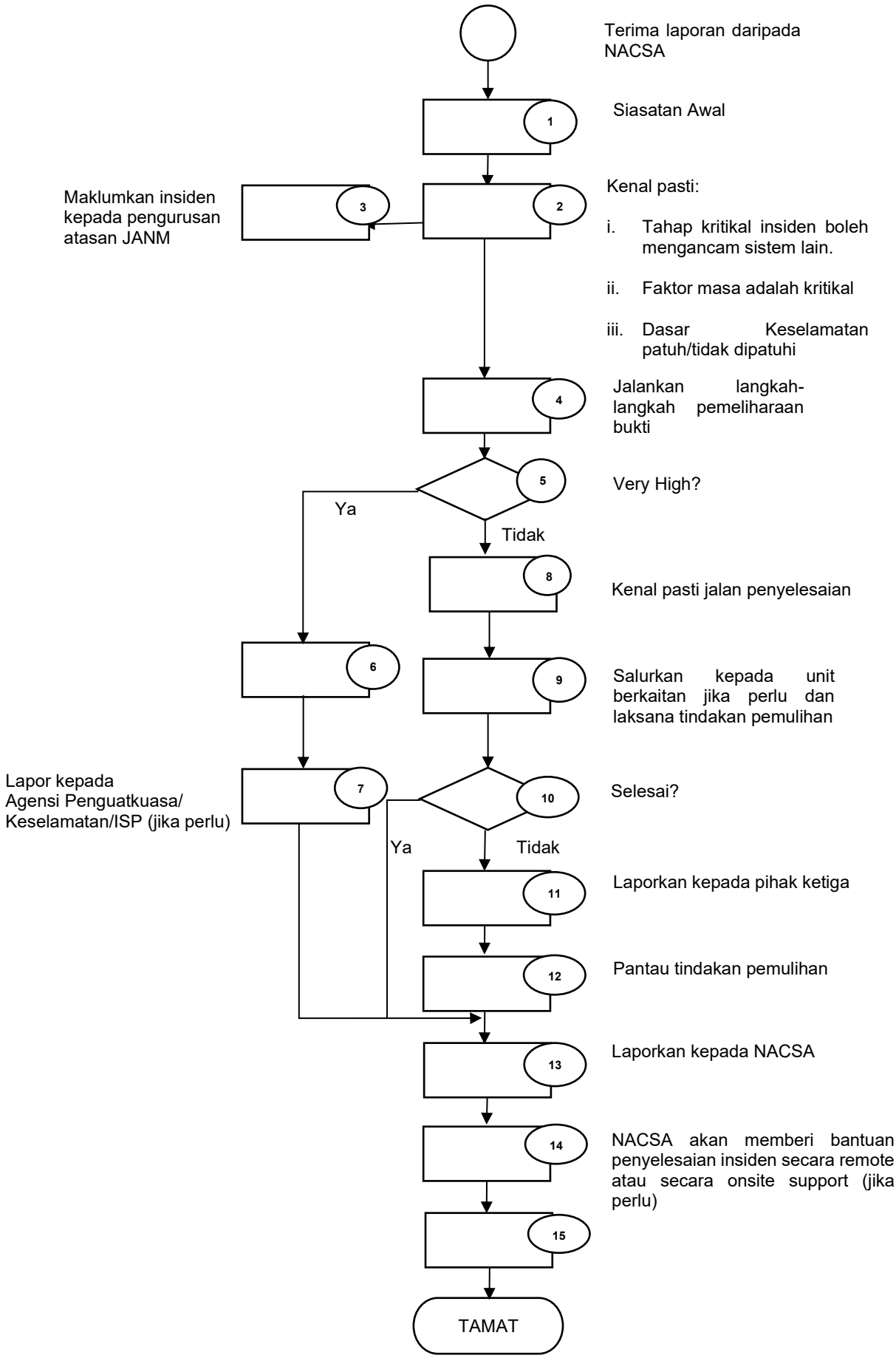
Jawatan Pegawai Pengesah :

Tarikh : .....

Nota: Pengesah adalah terdiri daripada CDO, ICTSO, Pengurus ICT atau Pentadbir Rangkaian dan Keselamatan.

**Peranti perkomputeran peribadi terdiri daripada komputer desktop, komputer riba, tablet, telefon pintar, thumb drive, smartwatch dan lain-lain peralatan ICT yang berkaitan

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT JANM



Lampiran 4

SENARAI PERUNDANGAN DAN PERATURAN

1) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

2) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;

3) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

4) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

5) Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

6) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

7) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;

8) Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran yang bertarikh 31 Januari 2007;

9) Surat Arahan Ketua Pengarah JDN - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

10) Surat Arahan Ketua Pengarah JDN - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

11) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

12) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

13) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

14) Akta Tandatangan Digital 1997;

15) Akta Rahsia Rasmi 1972;

16) Akta Jenayah Komputer 1997;

17) Akta Hak Cipta (Pindaan) Tahun 1997;

18) Akta Komunikasi dan Multimedia 1998;

19) Garis Panduan Keselamatan JDN 2004;

20) *Standard Operating Procedure* (SOP) ICT JDN;

21) Perintah-Perintah Am;

22) Arahan Keselamatan;

23) Arahan Perbendaharaan;

24) Arahan Teknologi Maklumat 2007;

25) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

26) Surat Arahan Ketua Pengarah JDN – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;

27) Surat Arahan Ketua Pengarah JDN – Pelaksanaan Pensijilan MS ISO/IEC Dalam Sektor Awam yang bertarikh 24 November 2010;

28) Pekeliling Kemajuan Pentadbiran Awam, Bilangan 1 Tahun 2021 - Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam (2.2.1 dan 2.2.2);

29) Pekeliling Pendigitalan Perkhidmatan Awam (PPPA) Bilangan 4 Tahun 2025 – Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan (Government Public Key Infrastructure – MyGPKI) yang bertarikh 12 Ogos 2025;

30) Akta Keselamatan Siber 2024 (Akta 854);

31) Cyber Security Code of Practice For National Critical Information Infrastructure (NCII) Entities Designated by The Ministry of Finance Under The Banking and Finance NCII Sector; dan

32) Arahan Ketua Eksekutif NACSA No. 9 – Penyediaan Data dan Maklumat Pelaksanaan Migrasi Kriptografi Pasca Kuantum Oleh Entiti Infrastruktur Maklumat Kritikal Negara.