DASAR KESELAMATAN ICT AGENSI PENGURUSAN BENCANA NEGARA (NADMA MALAYSIA)

AGENSI PENGURUSAN BENCANA NEGARA (NADMA)

Versi 1.0

A. INFORMASI DOKUMEN

Jenis Dokumen:	**Versi Dokumen :**	**Tarikh Berkuatkuasa:**
Manual Keselamatan	1.0	4 Ogos 2017
Disediakan Oleh :	**Disemak Oleh :**	**Diluluskan Oleh :**
Urusetia DKICT NADMA	Ketua Seksyen ICT	Mesyuarat Keselamatan ICT NADMA Bil 1/2017
Pengedaran Dokumen Seksyen ICT		

B. REKOD PINDAAN

KELUARAN / PINDAAN	TARIKH	KETERANGAN RINGKAS PINDAAN	BAB / MUKA SURAT	DILULUSKAN OLEH
1.0	04/08/2017	Penyediaan Dasar Keselamatn ICT (DKICT) dengan merujuk kepada Standard ISO/IEC 27001:2013 (Information Security Management System)		Jawatankuasa Keselamatan ICT Bil 1/2017

KANDUNGAN **HALAMAN**

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) Agensi Pengurusan Bencana Negara (NADMA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna di NADMA mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di NADMA.

2.0 TUJUAN

DKICT ini mengandungi peraturan-peraturan berkaitan penggunaan sumber ICT NADMA yang perlu dipatuhi oleh kakitangan NADMA, pengguna dan pembekal yang memberikan perkhidmatan. Tujuan DKICT ini disediakan adalah untuk menerangkan tanggungjawab dan peranan kakitangan NADMA, pengguna dan pembekal.

3.0 OBJEKTIF

Dasar Keselamatan ICT NADMA diwujudkan untuk menjamin kesinambungan urusan NADMA dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Dasar Keselamatan ICT NADMA ialah seperti berikut :

(a) Memastikan kelancaran operasi NADMA dan meminimumkan kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan, dan kesahihan (CIA);

(c) Mencegah salah guna atau kecurian aset ICT NADMA;

(d) Memperkemaskan pengurusan risiko; dan

(e) Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

4.0 PERNYATAAN DASAR KESELAMATAN ICT NADMA

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Pengurusan 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 bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. 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.

Dasar Keselamatan ICT NADMA merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan 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 kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) **Tidak Boleh Disangkal**

- Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal;

(e) **Kesahihan**

- Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) **Ketersediaan**

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

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

5.0 SKOP

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

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

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan NADMA.

Bagi memastikan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT NADMA ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan

sistem kawalan dan prosedur dalam pengendalian semua perkara- perkara berikut:

(a) **Perkakasan**

Semua aset yang digunakan untuk pemprosesan maklumat, kemudahan storan dan peralatan sokongan. Contoh komputer, pelayan, peralatan komunikasi, pencetak, *Uninterruptible Power Supply* (UPS), punca kuasa dan sebagainya;

(b) **Perisian**

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti Sistem MyDIMS, Sistem ePasca Bencana dan sistem pengoperasian seperti Windows, LINUX dan perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

(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.
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) **Data atau Maklumat**

Semua data atau maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

(e) **Media Storan**

Semua media storan dan peralatan yang berkaitan seperti storan mudah alih, CD-ROM, pemacu pita, pemacu cakera, pita *backup* dan lain-lain.

(f) **Dokumentasi**

Semua dokumen termasuk prosedur dan manual pengguna yang berkaitan dengan aset ICT, dokumen pemasangan dan pengoperasian peralatan dan perisian.

(g) **Premis Komputer dan Komunikasi**

Semua kemudahan serta premis yang diguna untuk menempatkan perkara (a) hingga (e) di atas.

(h) **Manusia**

Semua pengguna infrastruktur ICT NADMA yang dibenarkan termasuk kakitangan NADMA, pengguna dan pembekal.

6.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas Dasar Keselamatan ICT NADMA 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.;

(b) **Hak Akses Minimum**

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

(c) **Akauntabiliti**

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

(d) **Pengasingan**

Pengasingan hendaklah dilaksana bagi mengelakkan capaian yang tidak dibenarkan serta melindungi aset daripada kesilapan, kebocoran maklumat terperingkat atau manipulasi. Prinsip pengasingan hendaklah diamalkan dalam empat (4) keadaan berikut:

1) Infrastruktur

i) Rangkaian perlu dibezakan antara – LAN, WAN, VPN;
ii) Saluran komunikasi – *packet segmentation;* dan
iii) Platform aplikasi – *client server, web based atau stand alone.*

2) Persekitaran Pembangunan Sistem

Pengasingan dari segi persekitaran pembangunan sistem dilaksana berdasarkan persekitaran yang berikut:

i) Persekitaran Pembangunan;
ii) Persekitaran Pengujian; dan
iii) Persekitaran Pengoperasian

3) Kawalan Capaian

Pengasingan dari segi kawalan capaian terhadap aset dilaksana mengikut keperluan fungsi bidang tugas yang ditetapkan sama ada sebagai pengguna biasa atau pentadbir sistem.

4) Peranan dan Tanggungjawab

Pengasingan dari segi penyediaan dokumen dan kelulusan sesuatu permohonan dilaksana berdasarkan peranan dan tanggungjawab sebagai:

i) Penyedia atau pemohon;
ii) Penyemak atau penyokong; dan
iii) Pelulus.

(e) **Pengauditan**

Pengauditan melibatkan pemeliharaan semua rekod berkaitan tindakan keselamatan maklumat bagi mengenalpasti ancaman dan insiden berkaitan keselamatan. Semua aset yang terlibat hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit.

(f) **Pematuhan**

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

(g) **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan;

(h) **Tidak Boleh Disangkal**

Prinsip tidak boleh disangkal dilaksana bagi memastikan punca data dan maklumat adalah daripada punca yang sah dan tidak diragui; dan

(i) **Saling Bergantungan**

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

7.0 PENILAIAN RISIKO KESELAMATAN ICT

NADMA hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat. Justeru itu NADMA perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

NADMA hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/ atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat NADMA termasuklah aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses, dan 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.

NADMA bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

NADMA perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

2. Menerima dan/ atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;

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

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

BIDANG 01 DASAR KESELAMATAN	
0101 Pengurusan Keselamatan Maklumat ICT	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan NADMA dan perundangan yang berkaitan.	
010101 Dasar Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan NADMA kepada kakitangan NADMA, pengguna dan pembekal. **(A.5.1.1 *Policies for Information Security*)** Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah NADMA dibantu oleh Jawatankuasa Keselamatan ICT NADMA dan Jawatankuasa Keselamatan ICT NADMA yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh Ketua Pengarah.	Ketua Pengarah
0102 Kajian Semula Dasar Keselamatan Maklumat	
Dasar Keselamatan ICT NADMA perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan. **(A.5.1.2 *Review of policies for information security*)** Berikut adalah prosedur yang berhubung dengan kajian semula Dasar Keselamatan ICT NADMA. a) Mengenalpasti dan menentukan perubahan yang diperlukan;	ICTSO / JKICT

b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan Jawatan Kuasa Keselamatan ICT (JKICT) NADMA; (c) Memaklumkan cadangan pindaan yang telah dipersetujui oleh JKICT kepada JPICT bagi tujuan pengesahan; (d) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada semua kakitangan NADMA, pengguna dan pembekal; dan (e) Dasar ini hendaklah dikaji semula sekurang-kurangnya dua (2) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
0103 Pematuhan Dasar	
DKICT NADMA mestilah dipatuhi oleh semua kakitangan NADMA, pengguna dan pembekal.	Kakitangan NADMA, Pengguna, Pembekal

BIDANG 02 **KESELAMATAN ORGANISASI**	
0201 Struktur Organisasi Keselamatan	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT NADMA.	
020101 Ketua Pengarah	
Peranan dan tanggungjawab Ketua Pengarah NADMA adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT NADMA (c) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT NADMA; (d) Memastikan semua keperluan organisasi seperti sumber kewangan, sumber kakitangan dan perlindungan keselamatan adalah mencukupi; dan (e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT NADMA;	Ketua Pengarah
020102 Ketua Pegawai Maklumat (CIO)	

Jawatan Ketua Pegawai Maklumat (CIO) NADMA adalah disandang oleh Ketua Pengarah NADMA Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT NADMA; (c) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; (d) Menentukan keperluan keselamatan ICT; (e) Mempengerusikan Jawatankuasa Keselamatan ICT (JKICT); dan Memastikan program-program kesedaran mengenai Keselamatan ICT dilaksanakan;	CIO

020103 Pegawai Keselamatan ICT (ICTSO)	
Jawatan ICTSO bagi NADMA adalah disandang oleh Ketua Seksyen Teknologi Maklumat dan Komunikasi. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Mengurus keseluruhan program keselamatan ICT NADMA; (c) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT di NADMA; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT NADMA; (e) Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan *Malaysian Public Sector Management of Information and Communication* (MyMIS) untuk mengenalpasti ketidakpatuhan kepada DKICT NADMA; (f) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (g) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT	ICTSO

Kerajaan (GCERT MAMPU) dan seterusnya membantu dalam penyiasatan atau pemulihan; (h) Melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan Pelan Kesinambungan Perkhidmatan (PKP); (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (j) Memastikan pematuhan DKICT NADMA oleh pihak luar seperti pembekal dan kontraktor yang mencapai dan menggunakan aset ICT NADMA untuk tujuan penyelenggaraan dan sebagainya; (k) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan; dan (l) Memastikan Pelan Strategik ICT NADMA mengandungi aspek keselamatan;	

020104 Pengurus ICT	
Ketua Seksyen Teknologi Maklumat Komunikasi NADMA adalah merupakan Pengurus ICT NADMA. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan NADMA; (c) Menentukan kawalan akses pengguna terhadap aset ICT NADMA; (d) Melaporkan sebarang penemuan mengenai keselamatan ICT kepada JKICT NADMA ; (e) Menyimpan rekod atau laporan terkini tentang ancaman keselamatan ICT NADMA; (f) Memastikan semua kakitangan NADMA, kontraktor dan pembekal yang terlibat dengan aset ICT NADMA mematuhi dasar, piawaian dan garis panduan keselamatan ICT; (g) Melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: i. Pelaksanaan sistem atau aplikasi baru sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; ii. Pembelian atau peningkatan perisian dan sistem komputer; iii. Perolehan teknologi dan perkhidmatan komunikasi baru;	Pengurus ICT

iv. Menentukan pembekal dan rakan usahasama menjalani tapisan keselamatan.	
020105 Pentadbir Sistem	
Pegawai Teknologi Maklumat di setiap unit di Seksyen Teknologi Maklumat dan Komunikasi NADMA adalah merupakan Pentadbir Sistem ICT di NADMA. Pentadbir sistem terdiri seperti berikut : (i) Pentadbir Rangkaian dan Keselamatan; (ii) Pentadbir Pangkalan Data; (iii) Pentadbir Portal Rasmi NADMA (*Web Master*); (iv) Pentadbir Pusat Data; (v) Pentadbir Sistem Aplikasi; dan (vi) Pentadbir E-Mel.	Pentadbir Sistem
Pentadbir Rangkaian dan Keselamatan	
Peranan dan tanggungjawab Pentadbir Rangkaian dan Keselamatan adalah seperti berikut: (a) Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di NADMA beroperasi sepanjang masa; (b) Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; (c) Merancang peningkatan infrastruktur, ciri-ciri	Pentadbir Rangkaian dan Keselamatan

keselamatan dan prestasi rangkaian sedia ada; (d) Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; (e) Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; (f) Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian NADMA secara tidak sah seperti melalui peralatan modem dan *dial-up*; (g) Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; dan (h) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment*, SPA) serta penilaian risiko keselamatan maklumat.	
Pentadbir Pangkalan Data	
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: (a) Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; (b) Memastikan pangkalan data boleh digunakan pada setiap masa; (c) Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; (d) Memastikan aktiviti pentadbiran pangkalan data	Pentadbir Pangkalan Data

seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; (e) Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT; (f) Melaksanakan proses pembersihan data (*housekeeping*) di dalam pangkalan data; dan (g) Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
Pentadbir Portal/ Laman Web NADMA	
Peranan dan tanggungjawab Pentadbir Portal/ Laman Web NADMA adalah seperti berikut: (a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; (b) Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; (c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; (d) Menghadkan capaian Pentadbir Portal/ Laman Web ke *web server;* (e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal NADMA;	Pentadbir Portal/ Laman Web

(f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; (g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (h) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; (i) Melaksanakan proses *backup* dan *restore* secara berkala; dan (j) Melaporkan sebarang pelanggaran keselamatan laman portal kepada ICTSO.	
Pentadbir Pusat Data	
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: (a) Memastikan persekitaran fizikal dan keselamatan Pusat Data berada dalam keadaan baik dan selamat; (b) Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; (c) Menjadualkan dan melaksanakan proses salinan *(backup and restore)* ke atas pangkalan data secara berkala; (d) Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam DKICT; (e) Melaksanakan prinsip-prinsip DKICT; dan (f) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	Pentadbir Pusat Data

Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: (a) Mengkaji cadangan pembangunan/ penyelarasan sistem/ modul di NADMA; (b) Membuat kajian semula serta memperbaiki sistem/ modul sedia ada di NADMA; (c) Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem/ modul di NADMA; (d) Membuat pemantauan dan penyelenggaraan terhadap sistem / modul dari masa ke semasa; (e) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem/ modul; (f) Menyediakan dokumentasi sistem/ modul dan manual pengguna; (g) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (h) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; (i) Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggodam; (j) Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pewujudkan akaun pengguna ke atas setiap sistem aplikasi;	Pentadbir Sistem Aplikasi

(k) Melaksanakan sandaran (*backup*) sistem aplikasi pangkalan data yang berkaitan dengannya dibuat secara berjadual; (l) Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan daripada penyalahgunaannya; (m) Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; dan (n) Menjadi ahli Jawatankuasa Keselamatan ICT NADMA (JKICT).	
Pentadbir E-mel	
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: (a) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; (b) Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; (c) Memastikan akaun e-mel pengguna sentiasa di dalam keadaan baik dan berfungsi; (d) Memaklumkan kepada ICTSO sekiranya mengalami	Pentadbir E-mel

insiden keselamatan seperti serangan *virus*, serangan *e-mail spamming, phishing,* pencerobohan e-mel dan penyalahgunaan e-mel; (e) Pentadbir e-mel hendaklah mengurus dan menangani insiden yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih; (f) Menyediakan ruang *mailbox* yang mencukupi sekurang-kurangnya 200MB untuk setiap akaun emel dan jumlah ini adalah bergantung kepada keperluan pemilik akaun e-mel; (g) Memastikan pengguna e-mel NADMA berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel NADMA dan Internet NADMA serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan.	
020106 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (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 Dasar Keselamatan ICT NADMA dan menjaga kerahsiaan maklumat NADMA;	Pengguna

(e) Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. (f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (h) Menandatangani "Surat Akuan Pematuhan" (**LAMPIRAN 1**) bagi mematuhi Dasar Keselamatan ICT NADMA.	
020107 Jawatan Kuasa Keselamatan ICT NADMA	
Keanggotaan JKICT NADMA adalah seperti berikut:	CIO

Pengerusi: ICTSO (Pengarah Bahagian Khidmat Pengurusan)

Ahli :

- Ketua Seksyen ICT
- 2 Wakil setiap Bahagian
- Lain-lain ahli yang berkaitan mengikut keperluan

Urusetia: Seksyen ICT NADMA

Carta struktur organisasi JKICT NADMA seperti di **LAMPIRAN 2**.

Bidang Kuasa:

(a) Menyelenggara dokumen DKICT NADMA;
(b) Memantau tahap pematuhan DKICT NADMA;
(c) Menilai aspek teknikal keselamatan projek-projek ICT;
(d) Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT NADMA;
(e) Menyemak semula sistem ICT supaya sentiasa mematuhi keperluan keselamatan dari semasa ke semasa;
(f) Menilai teknologi yang bersesuaian dan

mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (g) Memastikan DKICT NADMA selaras dengan dasar-dasar ICT kerajaan semasa; (h) Bekerjasama dengan NADMACERT untuk mendapatkan maklum balas dan insiden untuk tindakan pengemaskinian DKICT NADMA; dan (i) Membincang tindakan yang melibatkan pelanggaran DKICT NADMA.	
020108 Pasukan Tindak Balas Insiden Keselamatan ICT NADMA (NADMACERT)	
Keanggotaan NADMACERT adalah seperti berikut: **<u>Pengerusi:</u>** Ketua Seksyen ICT NADMA **<u>Ahli :</u>** • Ketua Penolong Pengarah di Seksyen ICT NADMA • Pegawai Teknologi Maklumat di Seksyen ICT NADMA **<u>Urusetia:</u>** Seksyen ICT NADMA **<u>Bidang Kuasa</u>:** (a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (*response*) insiden	Pengarah BTMK

keselamatan ICT dan mengambil tindakan baik pulih minimum;

(d) Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya;

(e) Menasihati NADMA untuk mengambil tindakan pemulihan dan pengukuhan;

(f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan;

(g) Mengguna pakai *Standard Operating Procedure* (SOP) bagi pengurusan pengendalian insiden keselamatan; dan

(h) Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada ICTSO.

020109 Jawatankuasa Pemandu ICT (JPICT) NADMA	
Keanggotaan JPICT NADMA adalah seperti berikut: **Pengerusi:** Ketua Pengarah **Ahli :** • Timbalan Ketua Pengarah • Ketua Pegawai Maklumat (CIO) NADMA • Pengarah – pengarah Bahagian • Ketua Seksyen ICT • Lain-lain ahli yang berkaitan mengikut keperluan **Urusetia:** Seksyen ICT NADMA **Bidangkuasa:** (a) Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT NADMA; (b) Merancang, menyelaras dan memantau pelaksanaan program/projek ICT NADMA; (c) Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Teknologi Maklumat (ISP) NADMA; (d) Meluluskan projek-projek ICT; (e) Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; (f) Merancang dan menentukan langkah-langkah	Ketua Pengarah

keselamatan ICT; (g) Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT NADMA kepada Jawatankuasa Teknikal ICT Sektor Awam (JTISA) MAMPU untuk kelulusan; (h) Mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTISA NADMA; dan (i) Menetapkan dasar dan prosedur pengurusan portal rasmi NADMA.	
020110 Jawatankuasa Pelaksana MS ISO/IEC 27001:2013 Pengurusan Sistem Keselamatan Maklumat (ISMS) NADMA	

Keanggotaan jawatankuasa adalah seperti berikut: **<u>Pengerusi</u>:** ICTSO (Pengarah Bahagian Khidmat Pengurusan) **<u>Ahli</u> :** • Ketua Seksyen ICT • 2 Wakil setiap Bahagian • Lain-lain ahli yang berkaitan mengikut keperluan **<u>Urusetia:</u>** Seksyen ICT, NADMA **<u>Bidang Kuasa:</u>** (a) Merancang dan menyelaras struktur organisasi ISMS; (b) Menghadiri kursus kesedaran ISMS; (c) Menyediakan skop ISMS; (d) Menyediakan penyataan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *Risk Treatment Plan(RTP)*, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; (e) Mengemukakan isu dan masalah ISMS, sekiranya ada; dan (f) Mengukur keberkesanan kawalan ISMS.	Jawatankuasa Pelaksana ISMS

020111 Keperluan Keselamatan Kontrak dengan Pihak Luar/ Asing	
Memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/asing dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; (d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luar/ asing; (e) Perjanjian yang dimeterai perlu mematuhi perkara-perkara berikut : (i) Dasar Keselamatan ICT NADMA; (ii) Tapisan Keselamatan; (iii) Perakuan Akta Rahsia Rasmi 1972; (iv) Hak Harta Intelek; dan (v) Arahan Teknologi Maklumat. (f) Capaian kepada aset ICT NADMA perlu berlandaskan kepada perjanjian kontrak atau lain-lain persetujuan bertulis yang diberikan oleh NADMA; (g) Menandatangani Surat Akuan Pematuhan DKICT	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Luar/ Asing.

NADMA seperti di **LAMPIRAN 1;** (h) Pihak luaran (pembekal, kontraktor, perunding dan sebagainya) juga perlu menandatangani Borang KPKK 11 dan *Declaration To Be Signed By Contractors, Official Secrets Act* (OSA) 1972 bagi perakuan untuk tidak membocorkan sebarang maklumat rasmi yang diperolehi sepanjang berkhidmat dengan NADMA.	

BIDANG 03 KESELAMATAN SUMBER MANUSIA	
0301 Sebelum Perkhidmatan	
Objektif: Memastikan kakitangan NADMA dan pihak luar seperti pembekal dan pakar runding memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.	
030101 Tapisan Keselamatan (*Screening*)	
Menjalankan tapisan keselamatan terhadap kakitangan NADMA, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan. **(A.7.1.1 *Screening*)**.	Semua
030102 Terma dan Syarat	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab kakitangan NADMA, pembekal, pakar runding dan pihak- pihak lain yang terlibat dalam menjamin keselamatan aset ICT; dan (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. **(A.7.1.2 *Terms and Conditions Of Employment*)**.	Semua
0302 Dalam Perkhidmatan	
Memastikan kakitangan NADMA dan pihak luar seperti pembekal dan pakar runding mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua kakitangan NADMA dan pihak luar hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat	

kuasa.	
030201 Tanggungjawab Pengurusan	
(a) Memastikan kakitangan NADMA, pembekal dan pakar runding mematuhi dasar keselamatan maklumat NADMA; dan (b) Memastikan kakitangan NADMA, pembekal dan pakar runding mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh NADMA. **(A.7.2.1 *Management responsibilities*).**	Semua
030202 Latihan kesedaran dan Pendidikan Keselamatan Maklumat	
Kakitangan NADMA, pembekal dan pakar runding perlu diberikan program kesedaran mengenai keselamatan ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. **(A.7.2.2 *Information security awareness, education and training*).**	Semua
030203 Tindakan Tatatertib	
(a) Memastikan adanya proses tindakan disiplin dan /atau undang-undang ke atas kakitangan NADMA sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh NADMA;	Semua

(b) Pengguna yang melanggar DKICT NADMA akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT NADMA. **(A.7.2.3 *Disciplinary process*)**	
0303 Bertukar Atau Tamat Perkhidmatan	
Objektif: Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas kakitangan NADMA diurus dengan teratur.	
030301 Tamat Perkhidmatan Atau Perubahan Bidang Tugas	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikembalikan kepada NADMA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan NADMA dan terma perkhidmatan yang ditetapkan. **(A.7.3.1 *Termination or change of employment responsibilities*).**	Semua

BIDANG 04 PENGURUSAN ASET	
0401 Akauntabiliti/Tanggungjawab Aset	
Objektif: Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT NADMA.	
040101 Inventori Aset	
Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT NADMA. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) Memastikan semua aset ICT dikenal pasti, dikelas (dikategori), didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Inventori sebagaimana mengikut Pekeliling Perbendaharaan Bil.5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA); **(A.8.1.1 *Inventory of assets*)** dan **(A.8.1.2 *Ownership of assest*)** dan **(A.8.1.3 Acceptable use of assests**). (c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (d) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di NADMA; (e) Memastikan semua peraturan pengendalian aset dikenalpasti, didokumenkan dan dilaksanakan; dan (f) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset dan Pengguna

(A.8.1.2 *Ownership of assest*). (g) Semua pengguna NADMA hendaklah memulangkan semua aset kepada NADMA selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak. **(A8.1.4 *Return of assests*).** (h) Semua aset sewaan haruslah dipelihara dengan baik oleh pemegang aset.	
0402 Klasifikasi Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	
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.8.2.1 *Classification guidelines*).** (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Semua

040202 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang digunapakai oleh NADMA. A.8.2.2 (***Labelling of information***)	Semua
040203 Pengendalian Aset	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : **(A.8.2.3 *Handling of assets*).** (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

0403 Pengendalian Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Pengurusan Media Mudah Alih (*Removal* Media)	
Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh NADMA. **(A.8.3.1 Management of removal media**) Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua media di tempat yang selamat.	CIO, Pegawai Teknologi Maklumat dan Pengguna
040302 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dari pihak pengurusan ICT dan mengikut prosedur NADMA yang mana berkenaan. (A.8.3.2 ***Disposal Media***).	CIO, Pegawai Teknologi Maklumat dan Pengguna

Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran NADMA.	
040303 Pemindahan Media Fizikal	
NADMA hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan. **(A.8.3.3 *Physical media in transit*)**.	Semua

BIDANG 05 **KAWALAN CAPAIAN**	
0501 Keperluan Kawalan Capaian	
Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Dasar Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. **(A.9.1.1 *Access control policy*)** Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan keselamatan aplikasi NADMA; (b) Kebenaran untuk menyebarkan maklumat; (c) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; (d) Undang-undang Malaysia/ Persekutuan yang berkaitan dan obligasi kontrak mengenai had akses kepada data atau perkhidmatan; (e) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;	ICTSO, Pengurus ICT dan Pentadbir Sistem

(f) Pengasingan peranan kawalan capaian; (g) Kebenaran rasmi permintaan akses; (h) Keperluan semakan hak akses berkala; (i) Pembatalan hak akses; (j) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan (k) Akses *privilage.*	
050102 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari ICTSO. **(A.9.1.2 *Access to network and network services*)** Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian NADMA, rangkaian agensi lain dan rangkaian awam; (b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO, Pengurus ICT dan Pentadbir Rangkaian dan Keselamatan

0502 Pengurusan Capaian Pengguna	
Objektif: Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	
050201 Pendaftaran Pengguna dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian (A.9.2.1 ***User registration and deregistration***). Perkara –perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh NADMA sahaja boleh digunakan; (b) Akaun pengguna mestilah unik; (c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada NADMA terlebih dahulu; (d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan NADMA.	Pengguna NADMA, Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT

050202 Penyediaan Akses Pengguna (*Provisioning*)	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT **(A.9.2.2 *User access provisioning*)**	Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
050203 Pengurusan Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas. **(A.9.2.3 *Management of Privileged Access Rights*).**	Pentadbir Sistem Aplikasi
050204 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan dalam NADMA. (A.9.2.6 ***Removal or adjustment of access rights***)	Pentadbir Sistem Aplikasi, Pentadbir e-mel, ICTSO, Pengurus ICT
0503 Tanggungjawab pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a)Membaca, memahami dan mematuhi Dasar Keselamatan ICT NADMA; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT NADMA dan menjaga kerahsiaan maklumat	Pengguna, Pentadbir Sistem, ICTSO, Pengurus ICT

NADMA; (d) Melaksanakan langkah-langkah perlindungan seperti berikut :- • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia untuk digunakan; • Menjaga kerahsiaan kata laluan; • Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; • Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan • Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. (e)Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT.	

050301 Penggunaan Kata Laluan	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahihan identiti. **(A.9.3.1 *Use of secret authentication information*)**	Pengguna, Pentadbir Sistem, ICTSO, Pengurus ICT
0504 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
050401 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian. **(A.9.4.1 *Information access restriction*)**	Pengguna, Pentadbir Sistem, ICTSO, Pengurus ICT
050402 Prosedur *Log-on*	
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan *log-on* yang bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. **(A.9.4.2 *Secure log-on procedure*)**. Kaedah-kaedah yang digunakan adalah seperti berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; (b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses *log-on* terhadap aplikasi	Pentadbir Sistem, ICTSO, Pengurus ICT

sistem; (c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur *log-on* yang terjamin; (d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; (e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; (f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
050403 Sistem Pengurusan Kata Laluan	
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh NADMA seperti berikut: **(A.9.4.3 *Password Management System***) (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang kurangnya dua belas (12) aksara dengan gabungan antara huruf, aksara khas dan nombor (alphanumerik); (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun;	Pengguna, Pentadbir Sistem, ICTSO, Pengurus ICT

(e) Kata laluan *windows* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam aturcara; (g) Kuatkuasakan pertukaran katalaluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Had kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula;dan (j) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
050404 Penggunaan Utiliti Sistem	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem. **(A.9.4.4 *Use of privileged utility programs*)**	Pentadbir Sistem, ICTSO, Pengurus ICT

050405 Kawalan Akses Kepada *Source Code Program*	
Pembangunan sistem secara *outsource* perlu diselia dan dipantau oleh NADMA. **(A.9.4.5 *Access control to program source code***). (a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; (c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hakmilik NADMA.	Pentadbir Sistem, ICTSO, Pengurus ICT

BIDANG 06 KRIPTOGRAFI	
0601 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Kawalan Pengunaan Kriptografi	
Melindungi kerahsiaan, integriti dan kesahihan maklumat yang merangkumi data di dalam sistem rangkaian, sistem aplikasi dan pangkalan data. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut. **(A.10.1.1 *Policy on the use of cryptographic control*)** Kriptografi turut merangkumi kaedah-kaedah seperti berikut: (a) **Enkripsi** Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (encryption). (b) **Tandatangan Digital** Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. (c) **Pengurusan Infrastruktur Kunci Awam/Public Key Infrastructure (PKI)**	Pentadbir Sistem ICT

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

BIDANG 07 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0701 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat NADMA.	
070101 Kawalan Kawasan	
Ini bertujuan untuk menghalang capaian, kerosakan dan gangguan secaraperolehan fizikal terhadap premis dan maklumat agensi. **(A.11.1.1 *Physical security parameter*)** Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Menggunakan keselamatan perimeter (halangan seperti dinding,pagar,kawalan,pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan ; (d) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana disebabkan oleh kuasa Tuhan atau perbuatan manusia; (e) Melaksana perlindungan fizikal dan menyediakan	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, CIO

garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; (f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera;	
070102 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis NADMA. Perkara yang perlu dipatuhi adalah seperti berikut: **(A.11.1.2 *Physical entry controls***) (a) Setiap pegawai dan kakitangan NADMA hendaklah mempamerkan Pas Keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada NADMA apabila bertukar, tamat perkhidmatan atau bersara; (b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan (c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT NADMA; (d) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa.	Semua

070103 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: **(A.11.1.3 *Securing offices,rooms and facilities)*** (a) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh orang luar; (b) Penunjuk ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Semua
070104 Perlindungan Terhadap Ancaman Luaran dan Dalaman	
NADMA perlu merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana. **(A.11.1.4 *Protecting against external and environmental threats*)**	Semua
070105 Kawalan Tempat Larangan (*Working In Secure Area*)	
Kawasan larangan lokasi ICT bagi NADMA ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga NADMA yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis tersebut. Kawasan larangan lokasi ICT NADMA adalah pusat data NADMA. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: **(A.11.1.5 *Working in secure areas*)**	Pentadbir Pusat Data, Pentadbir Keselamatan ICT

(a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran;

(b) Akses adalah terhad kepada warga NADMA yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

(c) Pemantauan dibuat menggunakan Closed-Circuit Television (CCTV) kamera atau lain-lain peralatan yang sesuai;

(d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;

(e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

(f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;

(g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;

(h) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;

(i) Memperkukuhkan dinding dan siling; dan

(j) Menghadkan jalan keluar masuk.

070106 Kawasan Penghantaran dan Pemunggahan	
NADMA hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. (A.11.1.6 ***Delivery and loading areas***)	Semua
0702 Keselamatan Peralatan ICT	
Objektif: Melindungi peralatan ICT NADMA dari kehilangan, kerosakan, kecurian dan disalahgunakan.	
070201 Keselamatan Peralatan/ Peralatan ICT	
Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: **(A.11.2.1 *Equipment sitting and protection*)** **(A.11.2.2 *Supporting utilities*)** (a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;	Semua

(e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas mediastoran yang digunakan; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna; (g) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (*Gen-Set*); (i) Semua alat sokongan perlu disemak dan dikemaskinikan dari masa kesemasa (sekurang-kurangnya setahun sekali); (j) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (l) Peralatan ICT yang hendak dibawa ke luar dari	

premis NADMA, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;

(m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;

(n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan yang berkuatkuasa;

(o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

(p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaikpulih;

(q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

(s) Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak BTMK; dan

(t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat dibawah jagaannya dan digunakan hanya urusan rasmi dan Jabatan sahaja.

070202 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselaatan yang perlu diambil adalah seperti berikut: **(A.11.2.3 *Cabling security***) (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir rangkaian

070203 Penyelenggaraan Peralatan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: A.11.2.4 (***Equipment maintenance***) (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset,Unit ICT NADMA

070204 Peralatan Dibawa Keluar Premis	
(a) Peralatan ICT yang hendak dibawa keluar dari premis NADMA untuk tujuan rasmi, perlulah mendapat kelulusan CIO atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan. (A.11.2.5 ***Removal of assests***)	Pengguna, Pegawai Aset dan Ketua Jabatan
070205 Keselamatan Peralatan di Luar Premis	
Peralatan yang dibawa keluar dari premis NADMA adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: **(A.11.2.6 *Security of equipment off-premises*)** (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua

070206 Pelupusan Peralatan dan Kitar Semula	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh NADMA dan ditempatkan di NADMA sendiri dan SMART. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan NADMA. Langkah-langkah seperti berikut hendaklah diambil: **(A.11.2.7 *Secure disposal or re-use of equipment*)** (a) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (e) Pengguna ICT adalah **DILARANG SAMA**	Pegawai Aset, Seksyen ICT NADMA

SEKALI daripada melakukan perkara-perkara seperti berikut :

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya.

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *speake*r dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di jabatan.

iii. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan dibawah tanggungjawab NADMA.

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

(g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;

(h) Sekiranya maklumat perlu disimpan, maka

pengguna boleh membuat salinan; (i) Maklumat lanjut berhubung pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan 5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA); (j) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara;dan (k) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori (Sistem Pengurusan Aset)	
070207 Perkakasan Tanpa Penyeliaan (*Unattended user equipment*)	
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: **(A.11.2.8 *Unattended User Equipment*)** (a) Tamatkan sesi aktif apabila selesai tugas; (b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; (c) Komputer meja, komputer riba atau pelayan disimpan dengan selamat daripada pengguna yang tidak dibenarkan.	Semua

070208 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. **(A.11.2.9 *Clear Desk and Clear Screen policy*)** Langkah-langkah perlu diambil termasuklah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat. (d) E-mel masuk dan keluar hendaklah dikawal; dan (e) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Semua

BIDANG 08 **PENGURUSAN OPERASI**	
0801 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.	
080101 Pengendalian Prosedur	
(a)Semua prosedur keselamatan ICT yang di wujud, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal; (b)Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluankapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c)Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan. **(A.12.1.1 *Documented operating procedures*)**	Semua
080102 Kawalan Perubahan	
(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara,	Pentadbir Sistem

menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak. **(A.12.1.2 *Change management*)**	
080103 Perancangan Kapasiti	
(a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan (b) 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. (A.12.1.3 ***Capasity management***)	Pentadbir Sistem, Pentadbir Emel, Pentadbir Pusat Data dan Pengurus ICT

080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
(a) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*). (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. **(A.12.1.4 *Separation of development, test and operational facilities*)**	Pentadbir Sistem, Pengurus ICT
0802 Perisian Berbahaya (*Protection from Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
080201 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah	Pentadbir Sistem, Pengguna

mana-mana undang-undang bertulis yang berkuatkuasa;

(c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;

(d) Mengemas kini antivirus dengan *pattern* antivirus yang terkini ;

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;dan

(h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.

(A.12.2.1 *Controls againts malware*)

0803 *Backup*	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
080301 Backup Maklumat (*Information Backup*)	
Memastikan sistem dapat dibangunkan semula setelah berlakunya bencana. *Backup* hendaklah dilakukan setiap kali berlakunya sebarang perubahan. *Backup* hendaklah direkodkan dan disimpan di *off site*. A.12.3.1 (***Information backup***) (a) Membuat salinan pendua ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem *backup* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	Pentadbir Sistem

0804 Log dan Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080401 Event logging	
Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut: (A.12.4.1 ***Event* logging**). i. Fail log sistem pengoperasian; ii. Fail log servis (contoh: web, e-mel); iii. Fail log aplikasi (audit trail); dan iv. Fail log rangkaian (contoh: switch, firewall, IPS). Pentadbir Sistem hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem

080402 Perlindungan Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan. **(A.12.4.2 *Protection of log information*)**	Pentadbir Pusat Data, Pentadbir Sistem, ICTSO
080403 Log pentadbir dan Operator	
(a) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa kesemasa dan menyediakan laporan jika perlu; (c) Kesalahan, kesilapan dan/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 Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO. (A.12.4.3 ***Administrator and operator logs***)	Pentadbir Sistem, ICTSO

080404 *Clock Synchronisation*	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam NADMA atau *network time zone* (NTP) perlu diselaraskan dengan satu sumber waktu yang ditetapkan oleh SIRIM. **(A.12.4.4 *Clock synchronization*)**	Pentadbir Pusat Data
0805 Kawalan Perisian Operasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem Operasi	
(a) Pengemaskinian perisian operasi, aplikasi dan *library program* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; (A.12.5.1 ***Installation of software on operational systems***). (b) Sistem operasi hanya boleh memegang "*executable code*"; (c) Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; (d) Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi. Konfigurasi hanya boleh	Pentadbir Sistem dan Pengurus ICT

dilaksanakan selepas mendapat persetujuan dari pihak berkaitan; (e) Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan;dan (f) Versi lama perisian perlu diarkibkan selaras dengan Pengurusan Rekod Elektronik, Jabatan Arkib Negara.	
0806 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan dari Ancaman Teknikal	
Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (A.12.6.1 ***Management of technical vulnerabilities***). (a) Memperoleh maklumat keterdedahan teknikal sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

080602 Kawalan Pemasangan Perisian	
(a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pengguna di NADMA; (A.12.6.2 ***Restriction on software installation***) (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 anti virus sebelum menggunakannya.	Pengguna,Pentadbir Sistem ICT, ICTSO
0807 Pertimbangan Audit Sistem Maklumat	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080701 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	
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. A.12.7.1 (***Information systems audit controls***)	Semua

BIDANG 09 PENGURUSAN KOMUNIKASI	
0901 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan perlindungan pemprosesan maklumat dalam rangkaian.	
090101 Kawalan Infrastruktur Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. **(A.13.1.1 *Network control*)** Perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (*FAC*) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;	Pengguna, Pentadbir Rangkaian dan ICTSO

(f) Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan BTMK,NADMA; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat NADMA; (i) Memasang *Web Content Filtering* pada Internet Gateway untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTMK, NADMA adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di NADMA sahaja dan penggunaan modem adalah dilarang sama sekali; (l) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya; (m)Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian NADMA, rangkaian agensi lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;	

(p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan NADMA; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan NADMA.	
090102 Keselamatan Perkhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. **(A.13.1.2 *Security of network services*)**	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
090103 Pengasingan rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian NADMA. **(A.13.1.3 *Segregation in networks)***	Pentadbir Rangkaian, Pengurus ICT dan ICTSO

0902 Pemindahan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara NADMA dan pihak luar terjamin.	
090201 Dasar dan Prosedur Pemindahan Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Terma pemindahan maklumat dan perisian di antara NADMA dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan (d) Memastikan maklumat yang terdapat dalam emel elektronik hendaklah dilindungi sebaik-baiknya. **(A.13.2.1 *Information transfer policies and procedures*)**	Semua Pengguna, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO
090202 Perjanjian Mengenai Pemindahan Maklumat	
NADMA perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara NADMA dengan pihak luar. Perkara yang perlu dipertimbangkan	CIO, ICTSO Pengurus ICT

adalah: **(A.13.2.2 *Agreements on information transfer*).** (a) Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi. (b) Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat. (c) Menggunapakai prinsip dan tatacara *escrow*. (d) Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	
090203 Pengurusan Mel Elektronik (E-mel)	
Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003 dan mana-mana undang-undang bertulis yang berkuat kuasa. **(A.13.2.3 *Elektronic messaging*)** Perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Menggunakan akaun atau alamat mel elektronik (e-mel) NADMA bagi urusan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap emel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh NADMA;	Semua

(c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; (f) Pengguna dilarang dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (g) Pengguna hendaklah mengenal pasti dan mengesahkan identity pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; (k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;	

(l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti *yahoo.com*, *gmail.com*, *streamyx.com.my* dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas penyelenggaraan *mailbox* masing-masing.	
090204 Kerahsiaan dan *Non-Disclosure Agreement*	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari masa ke semasa. **(A.13.2.4 *Confidentiality or non-disclosure agreements).***	CIO,ICTSO,Semua

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
1001 Keperluan Keselamatan Sistem Maklumat	
Objektif: Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Keperluan keselamatan maklumat bagi pembangunan sistem baru dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: **(A.14.1.1 *Information security requirements analysis and spesifications*)** (a) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Dasar Keselamatan ICT NADMA; (b) Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (c) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pentadbir Sistem

100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: **(A.14.1.2 *Securing application services on public networks*)** (a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); (b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; (c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan (d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Rangkaian dan Pentadbir Sistem
100103 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi	ICTSO, Pentadbir Rangkaian dan Keselamatan, Pentadbir Sistem

mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: **(A.14.1.3 *Protecting application services transactions*)** (a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan. ii. Mengekalkan kerahsiaan maklumat. iii. Mengekalkan privasi pihak yang terlibat. iv. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. (c) Pihak yang mengeluarkan tandatangan digital adalah dilantik oleh Kerajaan.	
1002 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: **(A.14.2.1 *Secure development policy*)**	Pentadbir Sistem, ICTSO

(a) Keselamatan persekitaran pembangunan (b) Keselamatan pangkalan data (c) Keselamatan dalam kawalan versi (d) Bagi pembangunan secara *outsource*, kebolehan pembekal untuk mengenalpasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem (sebelum penentuan pembekal)	
100202 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: **(A.14.2.2 *System change control procedures*)** (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 sesebuah unit tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh *vendor*; (c) Mengawal perubahan dan/atau pindaan ke atas pakej	Pentadbir Sistem, Pengurus ICT

perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan (d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
100203 Kajian Teknikal Selepas Permohonan Perubahan Platform	
Perkara yang perlu dipatuhi adalah seperti berikut: **(A.14.2.3 *Technical review of applications after operating platform changes*)** (a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. (c) Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan perkhidmatan (BCP).	Pentadbir Sistem
100204 Sekatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal. **(A.14.2.4 *Restrictions on changes to software packages*)**	Pentadbir Sistem, Pengurus ICT

100205 Prinsip Kejuruteraan Keselamatan Sistem (S*ecure System Engineering Principles)*	
Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasi, diselenggara dan digunapakai dalam pelaksanaan sistem. **(A.14.2.5 *Secure System Engineering Principles*)** Keselamatan perlu diambilkira dalam semua peringkat pembangunan sistem. Prinsip dan prosedur hendaklah sentiasa dikaji dari masa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	Pentadbir Sistem, Pengurus ICT
100206 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran pembangunan sistem (***development lifecycle***). **(A.14.2.6 *Secure development environment*)**	Pentadbir Sistem. Pengurus ICT
100207 Pembangunan Sistem Secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh Seksyen ICT NADMA. *Source code* adalah menjadi hak milik NADMA. **(A.14.2.7 Outsourced Software Development)**	Pentadbir Sistem, Pengurus ICT, ICTSO

100208 Pengujian Keselamatan Sistem	
(a) Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan; (b) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (c) Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti kesilapan maklumat; dan (d) Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan. **(A.14.2.8 *System security testing*)**	Pentadbir Sistem, ICTSO
100209 Penerimaan Pengujian Sistem	
Penerimaan pengujian semua sistem baru dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai. (A.14.2.9 ***System accepting testing***)	Pengguna, Pentadbir Sistem, ICTSO
1003 Data Ujian	
100301 Perlindungan Data Ujian	
(a) Data dan atur cara yang hendak diuji perlu dipilih, dilindungi dan dikawal. (b) Pengujian hendaklah dibuat ke atas atur cara yang terkini.	

(c) Mengaktifkan audit log bagi merekodkan aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. (***A.14.3.1 Protection of test data)***	

BIDANG 11 HUBUNGAN DENGAN PEMBEKAL	
1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan aset ICT NADMA yang boleh dicapai oleh pembekal dilindungi.	
110101 Dasar Keselamatan Maklumat Untuk Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset NADMA. Perkara yang perlu dipertimbangkan adalah seperti berikut: **(A.15.1.1 *Information security policy for supplier relationships*)** (a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; (b) Proses kitaran (*lifecycle)* yang seragam untuk menguruskan pembekal; (c) Mengawal dan memantau akses pembekal; (d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; (e) Jenis-jenis obligasi kepada pembekal; (f) Pelan kontigensi (***contingency plan***) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; (g) Latihan Kesedaran Keselamatan untuk NADMA kepada pembekal.	ICTSO, Pembekal

110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan NADMA. **(A.15.1.2 *Addressing security within supplier agreements*).**	Pembekal
110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambilkira keperluan keselamatan maklumat rantaian pembekal (*Supply Chain*) bagi menangani risiko. Perkara-perkara yang perlu diambilkira adalah seperti berikut: **(A.15.1.3 *Information and communication technology supply chain*).** (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa	ICTSO, Pembekal

semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
NADMA hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: **(A.15.2.1 *Monitoring and review supplier services*)** (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; (c) Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	ICTSO, Pembekal

110202 Pengurusan Perubahan Perkhidmatan Pembekal	
Perkara yang perlu diambilkira adalah seperti berikut: **(A.15.2.2 *Managing changes to supplier services*)** (a) Perubahan dalam perjanjian dengan pembekal; (b) Perubahan yang dilakukan oleh NADMA bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	ICTSO, Pembekal

BIDANG 12 **PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN**	
1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.	
120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. **(A.16.1.1 *Responsibilities and procedures*)**	ICTSO, Pengurus ICT dan NADMACERT
120102 Mekanisme Pelaporan Insiden	
Insiden keselamatan ICT atau ancaman yang mungkin berlaku ke atas aset ICT yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada ICTSO. Selepas itu ICTSO hendaklah melaporkan kepada GCERT MAMPU dengan kadar segera. **(A.16.1.2 *Reporting information security events*).** Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Maklumat didapati hilang, didedahkan kepada pihak-	ICTSO, Pengurus ICT dan NADMACERT

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-insiden yang tidak dijangka;

(h) Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di NADMA seperti di **LAMPIRAN 3**

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

(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.

120103 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat NADMA dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT **(A.16.1.3 *Reporting security weaknesses*)**	Semua
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat. **(A.16.1.4 *Assessment of and decision on information security events*)**	ICTSO
120105 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: **(A.16.1.5 *Response to information security incidents*)** (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian forensik sekiranya perlu;	ICTSO, NADMACERT

(c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (g) Menyediakan tindakan pemulihan segera; dan (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	
120106 Pengalaman Dari Insiden Keselamatan Maklumat	
Pengetahuan dan pengalaman yang diperolehi daripada menganalisis dan menyelesaikan kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa depan. **(A.16.1.6 *Learning from information security incidents*)**	ICTSO, NADMACERT
120107 Pengumpulan Bahan Bukti	
NADMA hendaklah menentukan prosedur untuk mengenalpasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti. **(A.16.1.7 *Collection of evidence*)**	ICTSO, NADMACERT

BIDANG 13 **Aspek keselamatan maklumat dalam Pengurusan Kesinambungan Perkhidmatan**	
1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Objektif:Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi	
130101 Rancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
NADMA hendaklah membangunkan pelan kesinambungan perkhidmatan dan mengenal pasti aspek keselamatan maklumat. **(A.17.1.1 *Planning information security continuity*)** Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi dan mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh CIO.	CIO, ICTSO
130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Pengurusan Kesinambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan (*stakeholder)* sistem penyampaian perkhidmatan dilindungi dan imej NADMA terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan NADMA di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Ketua Pengarah adalah bertanggungjawab untuk	CIO, ICTSO

memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT NADMA.

Pelan BCP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

(A.17.1.2 *Implementing information security continuity*)

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
(b) Senarai pegawai NADMA dan vendor berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan pegawai 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.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.

Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan pegawai yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

NADMA hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama NADMA hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara berikut perlu diberi perhatian:

(a) Mengenalpasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan;
(b) Mengenalpasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik;
(c) Mengenalpasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi;

(d) Mengenalpasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; (e) Menjalankan analisis impak organisasi; (f) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (g) Mendokumentasikan proses dan prosedur yang telah ditetapkan; (h) Mengadakan program latihan secara berkala kepada warga NADMA mengenai prosedur kecemasan; (i) Membuat *backup* mengikut prosedur yang ditetapkan; dan (j) Menguji, menyelenggara dan mengemaskini pelan keselamatan ICT sekurang-kurangnya setahun sekali. Pelan Kesinambungan Perkhidmatan (BCP) perlu dibangunkan dan hendaklah mengandungi perkara berikut: (a) Senarai keperluan keselamatan maklumat dalam membangunkan kesinambungan perkhidmatan; (b) Senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan; (c) Senarai personel NADMA dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai personel gantian juga hendaklah dikenalpasti bagi menggantikan personel yang tidak dapat hadir untuk menangani insiden;	

(d) Senarai lengkap maklumat yang perlu disalin pendua (*backup*) dan lokasi sebenar penyimpanannya; (e) Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; (f) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; (g) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; dan (h) Menguji tahap keselamatan kesinambungan perkhidmatan Salinan pelan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi organisasi untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. NADMA hendaklah memastikan salinan pelan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	

NADMA hendaklah mengkaji, mengesah dan menilai tahap keselamatan maklumat yang diwujudkan dan disimpan di lokasi kesinambungan perkhidmatan keselamatan. **(A.17.1.3 *Verify, review andevaluate information security continuity*)**	CIO, ICTSO
1302 *Redundancy*	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat NADMA perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa. Kemudahan pemprosesan maklumat NADMA perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa. **(A.17.2.1 *Availability of information process facilities*)**	ICTSO, BTMK

BIDANG 14 PEMATUHAN	
1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
140101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenalpasti dan dipatuhi oleh kakitangan NADMA dan pembekal. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di NADMA dan pembekal : **(A.18.1.1 *Identification of applicable legislation and contractual agreement*)** (a) Arahan Keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; (c) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); (d) Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai	Semua

Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; (f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; (g) Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam"; (h) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan PenerimaanTender"; (i) Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan"; (j) Akta Tandatangan Digital 1997; (k) Akta Rahsia Rasmi 1972; (l) Akta Jenayah Komputer 1997; (m) Akta Hak Cipta (Pindaan) Tahun 1997; (n) Akta Komunikasi dan Multimedia 1998; (o) Perintah-Perintah Am; (p) Arahan Perbendaharaan; (q) Arahan Teknologi Maklumat 2007; (r) *Standard Operating Procedure* (SOP) ICT NADMA; (s) Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam"; (t) Etika Penggunaan E-mel dan Internet NADMA; (u) Perintah-Perintah Am;	

(v) Arahan Perbendaharaan; (w) Surat Akujanji; (x) MPK; (y) Fail Meja Kakitangan; (z) Pelan Kesinambungan Perkhidmatan; (aa) Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk ”Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan”; (bb) Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk ”Penggunaan Media Jaringan Sosial di Sektor Awam”;Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)"; (cc) Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam; (dd) Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007"; dan (ee) Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT NADMA.	
140102 Hak Harta Intelek (*Intellectual Property Rights*-IPR)	
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta	Semua

intelektual. Melaksanakan kawalan terhadap keperluan perlesenan di mana mematuhi had pengguna yang telah ditetapkan atau dibenarkan dan hanya menggunakan perisian yang mempunyai lesen yang sah. **(A.18.1.2 *Intellectual property rights* (IPR)**	
140103 Perlindungan Rekod	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak. **(A.18.1.3 *Protection of records*)**	Semua
140104 Privasi dan perlindungan maklumat peribadi	
NADMA hendaklah memberi jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia. **(A.18.1.4 *Privacy and protection of personally identifiable information*)**	Semua

140105 Kawalan Kriptografi	
Kawalan kriptografi hendaklah dilaksanakan mengikut perundangan, peraturan dan perjanjian kontrak. **(A.18.1.5 *Regulation of cryptographic controls*)**	Semua
1402 Kajian Keselamatan Maklumat	
Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur NADMA.	
140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur. **(A.18.2.1 *Independent review of information security*)**	CIO
140202 Pematuhan Dasar dan Standard/Piawaian	
NADMA hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti di dalam polisi, piawaian dan keperluan teknikal. **(A.18.2.2 *Compliance with security policies and standards*)**	CIO

GLOSARI

Glosari	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CD ROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BCP	*Business Continuity Planning* Pelan Kesinambungan Perkhidmatan
CCTV	*Closed-circuit television system*

	Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
NADMACERT	Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CIA	*confidentiality, integrity, authenticity, accessibility, accountability*
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan si maklumat bagi menyokong arahtuju sesebuah organisasi.
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen, data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain

	kecuali penerima yang sah.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft / espionage*), penipuan(*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
ICT	*Information and Communication Technology*. (Teknologi Maklumat dan Komunikasi).

ICTSO	*ICT Security Office* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Kemalangan *(adverse event)* yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
ISDN	*Integrated Services Digital Networks* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.

Intrusion Detection Syatem (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
ISMS	*Information Security Management System*
NADMA	NADMA merangkumi bahagian-bahagian seperti berikut : • Sektor Pengurusan Pasca Bencana • Sektor Perancangan & Kesiapsagaan • Sektor Pelaksanaan Operasi • Bahagian Khidmat Pengurusan & Kewangan • Bahagian Komunikasi Korporat

Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Lock	Mengunci komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Mobile Code	*Mobile code* merupakan suatu perisian yang boleh dipindahkan diantara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses

	pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
MODEM	Modulator Demodulator Peranti yang boleh menukar *strim bit* digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuatkuasa.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan

	berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contoh: Capaian Internet.
Screen saver	Imej yang akan diaktifkan pada skrin komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan computer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya rangkaian diasingkan mengikut *segment*. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan sistem penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
WAN	Wide Area Network Rangkaian yang merangkumi kawasan yang luas.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Worm	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemaskini.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT NADMA

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT NADMA ; dan

3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

( ) Tarikh : .....

Pengesahan Pegawai Keselamatan ICT :

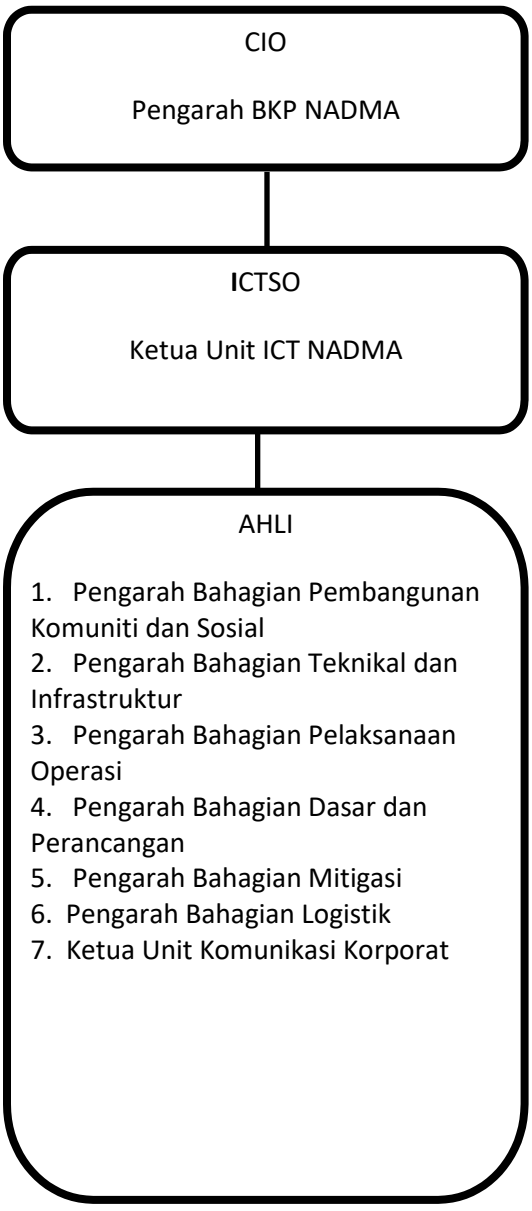
.....

( ) Tarikh : .....

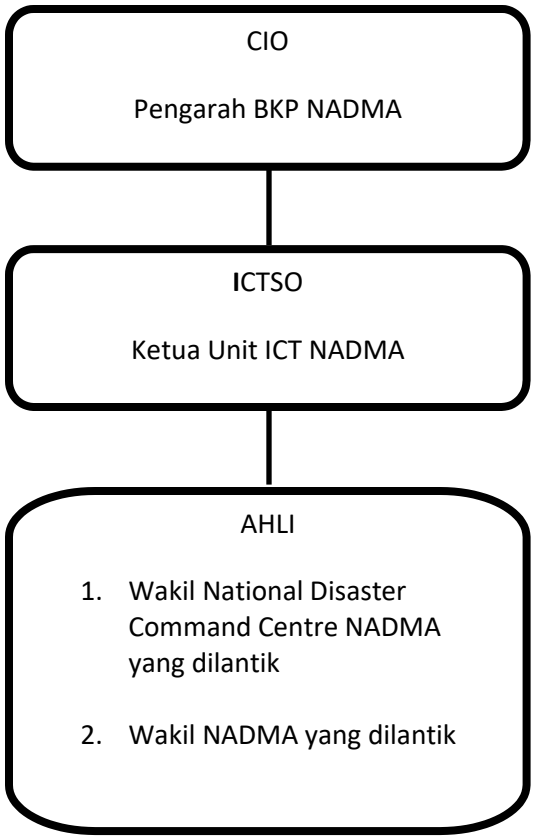
b.p Ketua Pengarah

LAMPIRAN 2

Carta 1 : Struktur Organisasi Jawatankuasa Keselamatan ICT NADMA

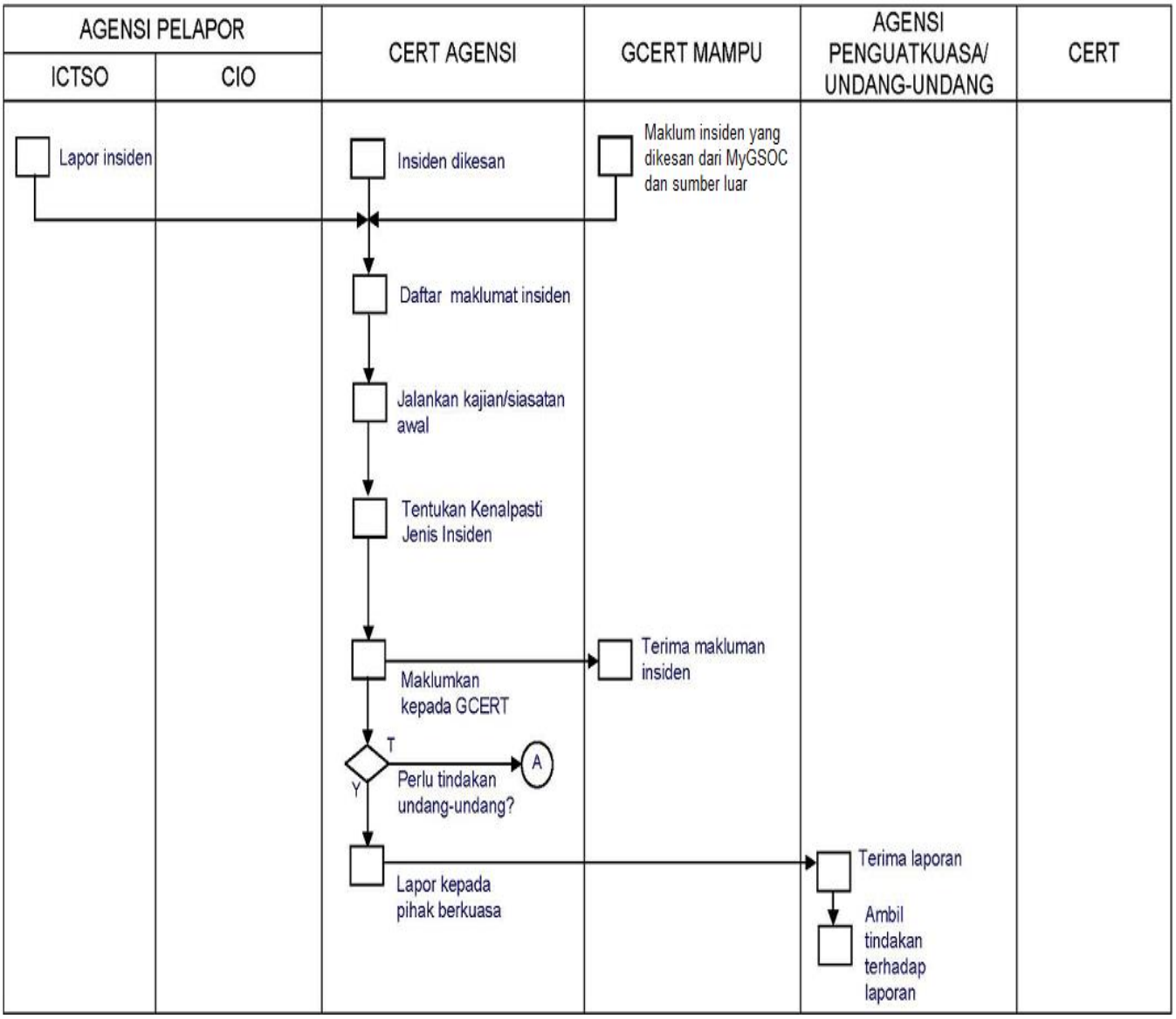


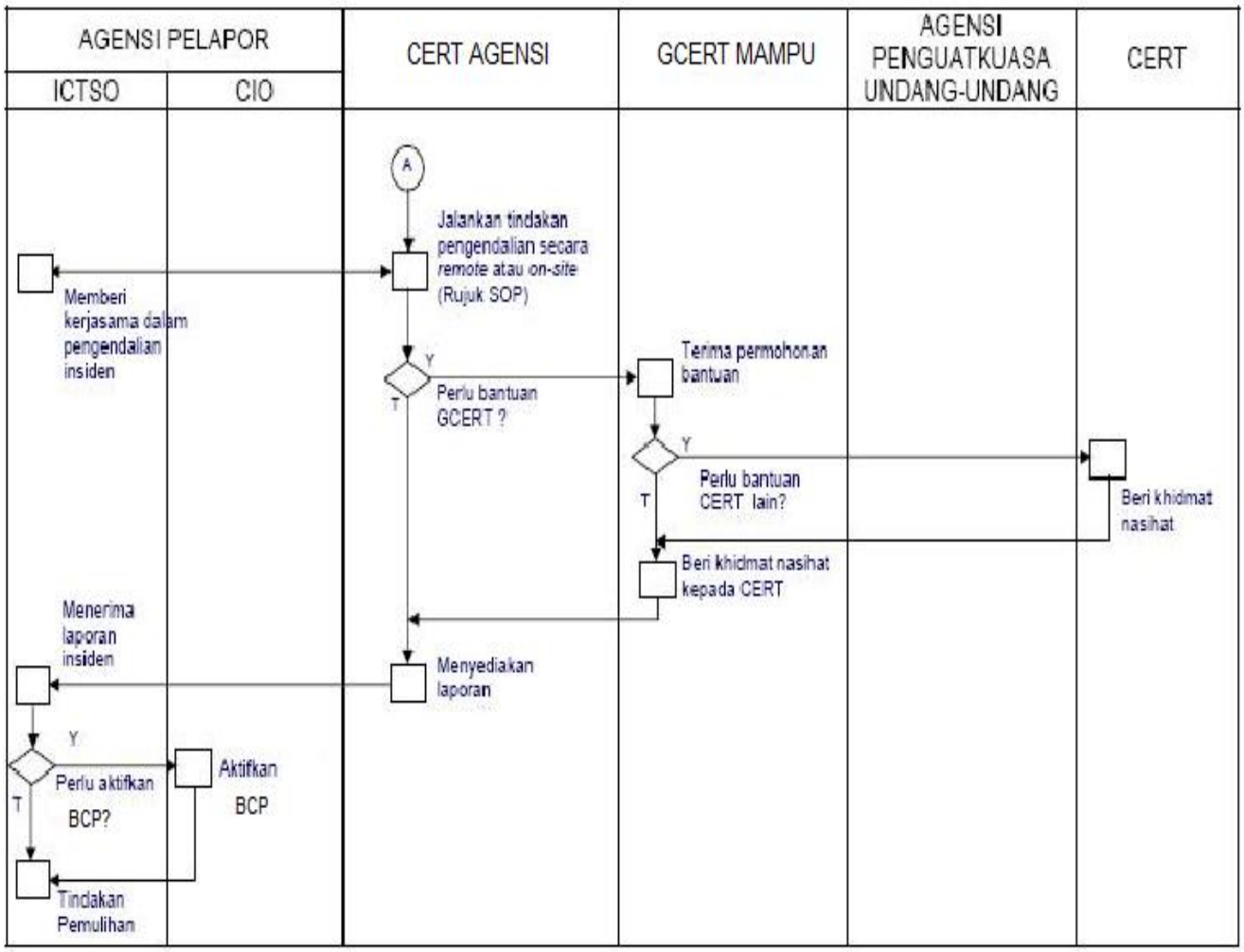
Carta 2 : Struktur Organisasi Jawatankuasa Kerja Keselamatan ICT NADMA



LAMPIRAN 3

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT NADMA




AGENSI PELAPOR
ICTSO
CIO
CERT AGENSI
GCERT MAMPU
AGENSI PENGUATKUASA UNDANG-UNDANG
CERT
A
Jalankan tindakan pengendalian secara remote atau on-site (Rujuk SOP)
Memberi kerjasama dalam pengendalian insiden
Y
T
Perlu bantuan GCERT ?
Terima permohonan bantuan
Y
T
Perlu bantuan CERT lain?
Beri khidmat nasihat
Beri khidmat nasihat kepada CERT
Menerima laporan insiden
Menyediakan laporan
Y
T
Perlu aktifkan BCP?
Aktifkan BCP
Tindakan Pemulihan