POLISI KESELAMATAN SIBER (PKS)

AGENSI ANTIDADAH KEBANGSAAN

KEMENTERIAN DALAM NEGERI

VERSI 1.0

TERBUKA

I. KELULUSAN DOKUMEN

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama : Junhairi bin Abu Noh	Nama : Razita binti Omar	Nama : Chan Hong Jin
Jawatan : Penolong Pegawai Teknologi Maklumat	Jawatan : Pengarah Teknologi Maklumat dan Komunikasi	Jawatan : Timbalan Ketua Pengarah (Pengurusan)
Tarikh : 14 Februari 2022	Tarikh : 21 Februari 2022	Tarikh : 28 Februari 2022

II. REKOD PINDAAN DOKUMEN

TARIKH	VERSI	BAB / MUKA SURAT	BUTIRAN PINDAAN
Februari 2022	1.0		Dokumen Asal

KANDUNGAN

A. PENGENALAN

Penggunaan teknologi maklumat dan komunikasi (ICT) untuk meningkatkan kecekapan dalam Penyampaian Perkhidmatan Kerajaan merupakan salah satu langkah dalam transformasi Sektor Awam di Malaysia. Ini bermakna maklumat atau data disimpan dan diproses dalam bentuk digital, atau dalam erti kata lain, dalam ruang siber. Justeru, pembangunan polisi keselamatan siber amat diperlukan sebagai panduan asas merangkumi komponen keselamatan yang perlu diambil kira oleh agensi sektor awam dalam melindungi maklumat dalam ruang siber mereka.

B. TUJUAN

Polisi Keselamatan Siber (PKS) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peratusan yang perlu difahami dan dipatuhi oleh warga AADK, pembekal, pakar runding atau sesiapa sahaja yang menggunakan perkhidmatan ICT Kerajaan dalam melindungi maklumat di ruang siber.

C. LATAR BELAKANG

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Pembangunan polisi keselamatan siber di agensi masing-masing berdasarkan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) perlu diambil kira bagi melindungi penyimpanan maklumat di ruang siber yang semakin meningkat dari semasa ke semasa.

PKS AADK dibangunkan untuk menjamin kesinambungan urusan AADK dengan meminimumkan kesan insiden keselamatan siber. Polisi ini juga memudahkan perkongsian maklumat sesuai dengan keperluan operasi AADK dengan memastikan semua maklumat dilindungi.

D. OBJEKTIF

Objektif utama pembangunan PKS AADK adalah seperti berikut:

(a) Menerangkan mengenai tanggungjawab dan peranan warga AADK, pembekal, pakar runding atau sesiapa sahaja yang menggunakan perkhidmatan ICT AADK dalam melindungi maklumat di ruang siber;

(b) Memastikan keselamatan penyampaian perkhidmatan AADK berada di tahap optimum bagi meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan dan orang awam;

(c) Memastikan kelancaran operasi AADK dan meminimumkan kerosakan atau kemusnahan berkaitan insiden keselamatan;

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

(e) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan ICT.

E. ASET ICT AADK

Aset ICT AADK merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

(a) Maklumat

Semua penyedia perkhidmatan di AADK hendaklah mengenai pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

i. Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

ii. Maklumat Rasmi

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

iii. Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (*PII* atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenai pasti individu tertentu. Data *PII* mengandungi data peribadi dan data sensitif individu. *PII* boleh juga terkandung dalam Maklumat Rahsia Rasmi.

iv. Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. *PII* dikecualikan daripada data terbuka.

(b) Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam AADK hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

i. Saluran komunikasi dan aliran data antara sistem di AADK;
ii. Saluran komunikasi dan aliran data ke sistem luar; dan
iii. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

(c) Platform Aplikasi dan Perisian

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

(d) Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

i. Pelayan;
ii. Peranti / Peralatan Rangkaian;

iii. Komputer Peribadi / Komputer Riba;
iv. Media Storan;
v. Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup *(CCTV)*;
vi. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan
vii. Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

(e) Sistem Luaran

Sistem luaran ialah sistem bukan milik AADK yang dihubungkan dengan sistem AADK. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

(f) Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi AADK. Contoh perkhidmatan sumber luaran ialah:

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

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

F. PENILAIAN RISIKO

AADK hendaklah mengenalpasti kewujudan risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian AADK tidak dapat melaksanakan fungsi jabatan dengan baik. AADK hendaklah melaksanakan penilaian risiko secara berkala dan berterusan bagi mengelakkan kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber AADK terjejas.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber AADK. Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

(a) Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

(b) Ancaman

AADK hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

(c) Impak

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

(d) Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

(e) Penguraian Risiko

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

ii. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

a. Teknologi

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

b. Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

c. Manusia

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

(f) Pengurusan Risiko

Penyedia perkhidmatan digital di AADK hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

i. mengenai pasti kerentanan;

ii. mengenai pasti ancaman;

iii. menilai risiko;

iv. menentukan penguraian risiko;

v. memantau keberkesanan penguraian risiko; dan

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

G. PRINSIP KESELAMATAN

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, AADK hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

(a) Akses atas dasar perlu mengetahui

AADK hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah 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 pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan / atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna / bidang tugas;

(c) Pengasingan Tugas

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan. AADK hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

(d) Kawalan Capaian Berdasarkan Peranan

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

(e) Peminimuman Data

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

H. MANUSIA

Warga AADK, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa. Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan.

(a) Peranan

i. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

ii. Pengguna yang terlibat dengan maklumat terperingkat adalah tertakluk kepada Akta Rahsia Rasmi 1972. Salinan perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

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

iv. Warga AADK yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

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

I. PERNYATAAN POLISI KESELAMATAN SIBER AADK

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat 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 dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan

Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan

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

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

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 01

POLISI KESELAMATAN MAKLUMAT

BIDANG 01: POLISI KESELAMATAN MAKLUMAT

0101 Hala Tuju Pengurusan Untuk Keselamatan Maklumat

Objektif :

Menjelaskan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan AADK dan perundangan yang berkaitan.

010101 Polisi Keselamatan Siber (PKS) AADK

PKS AADK ini dilaksanakan oleh Ketua Pengarah AADK dengan dibantu oleh ahli Jawatankuasa Pemandu ICT AADK (JICTA) serta pegawai-pegawai yang dilantik. PKS AADK ini perlu dipatuhi oleh warga AADK dan pihak ketiga seperti pembekal, kontraktor, pakar runding dan pihak yang berurusan dengan perkhidmatan ICT AADK.	Ketua Pengarah AADK / *CIO* / *ICTSO* / Pengarah Bahagian

010102 Kajian Semula Polisi

PKS AADK adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berkaitan dengan kajian semula PKS AADK: (a) Mengenal pasti dan menentukan perubahan yang diperlukan bagi memastikan dokumen adalah relevan; (b) Membentangkan cadangan pindaan PKS AADK dalam Mesyuarat JICTA bagi tujuan pertimbangan dan kelulusan; (c) Mengkaji semula PKS AADK setiap dua (2) tahun atau mengikut keperluan semasa.	*CIO* / *ICTSO*

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 02

PERANCANGAN BAGI KESELAMATAN ORGANISASI

BIDANG 02: PERANCANGAN BAGI KESELAMATAN ORGANISASI

0201 Perancangan Organisasi

Objektif:

Menerangkan peranan dan tanggungjawab semua pihak yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS AADK.

020101 Peranan dan Tanggungjawab Keselamatan Maklumat

02010101 Ketua Pengarah AADK

Peranan dan tanggungjawab Ketua Pengarah AADK adalah seperti berikut: (a) Memastikan penguatkuasaan pelaksanaan PKS AADK; (b) Memastikan warga AADK dan pihak ketiga memahami dan mematuhi peruntukan-peruntukan di bawah PKS AADK; (c) Memastikan semua keperluan AADK seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan; dan (e) Melantik *CIO* dan *ICTSO*.	Ketua Pengarah AADK

02010102 Ketua Pegawai Maklumat *(CIO)*

Ketua Pegawai Maklumat *(CIO)* bagi AADK ialah Timbalan Ketua Pengarah (Pengurusan) AADK. Peranan dan tanggungjawab *CIO* adalah seperti berikut: (a) Membantu Ketua Pengarah AADK dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan dalam PKS AADK; (b) Menyelaras keperluan keselamatan siber di AADK; dan (c) Menyelaras pelan latihan dan program kesedaran keselamatan siber.	*CIO*

02010103 Pegawai Keselamatan ICT *(ICTSO)*	
Pegawai Keselamatan ICT *(ICTSO)* bagi AADK ialah Pengarah Teknologi Maklumat dan Komunikasi (PTMK). Peranan dan tanggungjawab *ICTSO* yang dilantik adalah seperti berikut: (a) Menyelia pembangunan garis panduan / prosedur atau tatacara selaras dengan keperluan PKS AADK; (b) Memastikan pelaksanaan pengurusan risiko keselamatan maklumat di AADK; (c) Menyebarkan amaran terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (d) Melaporkan insiden keselamatan siber kepada *CIO* dan dipanjangkan kepada *CERT* Kementerian Dalam Negeri (KDN) berdasarkan tahap insiden; (e) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; (f) Memastikan pematuhan PKS AADK ini oleh warga AADK, pihak ketiga dan pihak yang mempunyai urusan dengan perkhidmatan ICT AADK; (g) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan (h) Menyedia dan merangka latihan dan program kesedaran keselamatan siber.	*ICTSO*

02010104 Pengurus ICT	
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Memastikan pelaksanaan PKS AADK secara berkesan dengan menyelaras pengwujudan garis panduan, prosedur dan tatacara selaras dengan keperluan keselamatan siber; (b) Mengurus pelaksanaan ujian penembusan dalaman dan luaran melibatkan sistem aplikasi dan rangkaian di AADK; dan (c) Melaksanakan dan mengemaskini penilaian risiko dan pelan penguraian risiko AADK.	Pengurus ICT
02010105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT terdiri daripada seperti berikut: (a) Pentadbir Pusat Data dan Rangkaian; (b) Pentadbir Sistem Aplikasi; dan (c) Pentadbir Laman Web.	Pentadbir Sistem ICT
02010106 Pentadbir Pusat Data dan Rangkaian	
Peranan dan tanggungjawab Pentadbir Pusat Data dan Rangkaian adalah seperti berikut: (a) Memastikan rangkaian setempat *(LAN)* dan rangkaian luas *(WAN)* di Ibu Pejabat AADK dan semua cawangan AADK beroperasi mengikut *Service Level Agreement (SLA)* yang ditetapkan; (b) Memastikan semua peralatan dan perisian rangkaian diselenggara; (c) Merancang peningkatan infrastruktur dan prestasi rangkaian sedia ada; (d) Mengambil tindakan pembaikan ke atas rangkaian yang tidak berfungsi; (e) Memantau penggunaan rangkaian dan melaporkan kepada *ICTSO* sekiranya berlaku penyalahgunaan sumber rangkaian;	Unit Pusat Data, Rangkaian dan Pemulihan Bencana ICT

(f) Memastikan tiada sambungan rangkaian yang tidak sah; dan (g) Menyediakan zon rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian jika berkaitan. (h) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; (i) Melaksanakan pemulihan bencana mengikut Pelan Pemulihan Bencana *(DRP)* ICT AADK; (j) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.	
02010107 Pentadbir Sistem Aplikasi	
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: (a) Menerima cadangan pembangunan sistem baru AADK menerusi Jawatankuasa ICT AADK (JICTA); (b) Membuat kajian semula ke atas cadangan yang diterima; (c) Membuat pemantauan dan penyelenggaraan terhadap sistem / modul sedia ada dari semasa ke semasa; (d) Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem / modul termasuk pangkalan data; (e) Menyediakan dokumentasi sistem / modul dan manual pengguna; (f) Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; (g) Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; (h) Memastikan *virus pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman virus dan penggodam; (i) Memastikan sandaran (*backup*) sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual;	Pentadbir Sistem Aplikasi

(j) Menghadkan capaian dokumentasi sistem aplikasi bagi mengelakkan dari penyalahgunaannya; dan (k) Melaporkan kepada *ICTSO* jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;	
02010108 Pentadbir Laman Web	
Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: (a) Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; (b) Mengambil tindakan pengukuhan sekiranya terdapat capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antar muka laman; (c) Memastikan reka bentuk *web* dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; dan (d) Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di pelayan web.	Unit Aplikasi Dalaman dan Laman Web
02010109 Pemilik Sistem	
Sesuatu sistem hendaklah dimiliki oleh Bahagian / Cawangan / Unit di AADK yang mempunyai kepentingan terhadap sistem yang dibangunkan. Pemilik Sistem adalah terdiri daripada Bahagian / Cawangan / Unit di AADK yang menggunakan sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: (a) Penentuan pengguna dan kategori atau tahap capaian pengguna sistem; (b) Pengurusan Latihan Pengguna dan penguatkuasaan penggunaan sistem; (c) Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan	Pemilik Sistem

(d) Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pentadbir Sistem ICT.	
02010110 Jawatankuasa Pemandu ICT AADK (JICTA)	
Jawatankuasa Pemandu ICT AADK (JICTA) adalah jawatankuasa yang bertanggungjawab dalam ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan projek ICT AADK. Keanggotaan JICTA adalah seperti berikut: **Pengerusi:** *CIO* AADK **Ahli:** 1. *ICTSO*; 2. Pengarah Khidmat Pengurusan; 3. Pengarah Penguatkuasaan & Keselamatan; 4. Pengarah Pencegahan; 5. Pengarah Rawatan, Perubatan & Pemulihan; 6. Pengarah Dasar, Perancangan & Penyelidikan; 7. Pengarah Pusat Latihan; 8. Pengarah Unit Integriti; 9. Pegawai Perhubungan Awam; 10. Ketua Unit MTMD; 11. Wakil Zon yang dilantik; 12. Penasihat Undang-undang (PUU); 13. Pegawai Kanan, Bahagian Teknologi Maklumat dan Komunikasi; 14. Lain-lain ahli yang berkaitan (mengikut keperluan).	JICTA

Bidang kuasa:

(a) Menetapkan hala tuju dan strategi untuk pelaksanaan ICT di AADK;

(b) Merancang, menyelaras dan memantau pelaksanaan program atau projek ICT AADK;

(c) Memantau perkembangan program ICT di AADK serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;

(d) Meluluskan perolehan ICT bagi AADK berdasarkan keperluan sebenar dengan perbelanjaan yang berhemah serta mematuhi pekeliling / peraturan semasa yang berkaitan; dan

(e) Menyelaras dan mengemukakan laporan perolehan ICT AADK kepada Urus Setia JPICT KDN mengikut tempoh yang telah ditetapkan.

02010111 Pasukan Tindak Balas Insiden Keselamatan ICT AADK *(CERT* AADK)

CERT AADK

Keanggotaan CERT AADK adalah seperti berikut:

Pengarah: Ketua Pegawai Maklumat *(CIO)*

Pengurus: Pegawai Keselamatan ICT *(ICTSO)*

Ahli:

1. Unit Aplikasi Teras (wakil yang dilantik);
2. Unit Keselamatan ICT (wakil yang dilantik);
3. Unit Teknikal dan Helpdesk (wakil yang dilantik);
4. Unit Pusat Data, Rangkaian dan Pemulihan Bencana ICT (wakil yang dilantik); dan
5. Unit Aplikasi Dalaman dan Laman Web (wakil yang dilantik).

Peranan dan tanggungjawab *CERT* AADK adalah seperti berikut:

(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 keselamatan ICT dan mengambil tindakan baik pulih minima; (d) Menghubungi dan melapor insiden yang berlaku kepada *NACSA* berdasarkan tahap keutamaan tindakan ke atas insiden samada sebagai input atau untuk tindakan seterusnya; dan (e) Menyebarkan makluman berkaitan pengukuhan keselamatan siber dan insiden kepada warga AADK.	
02010112 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti yang berikut: (a) Membaca, memahami dan mematuhi PKS AADK; (b) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya; (c) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada *CERT* AADK dengan segera; (d) Melaksanakan langkah-langkah perlindungan seperti yang 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 maklumat; • Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; • Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. (e) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (f) Bersetuju dengan terma dan syarat yang terkandung di dalam PKS AADK.	Warga AADK

0202 Pihak Ketiga	
Pihak ketiga terdiri daripada Kontraktor, Pembekal dan Penyedia Perkhidmatan Luaran. Peranan dan tanggungjawab Pihak Ketiga diperincikan bagi memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal seperti keperluan berikut: (a) Penjagaan kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; (b) Penjagaan kerahsiaan kata laluan dan kerahsiaan kawalan keselamatan siber dari diketahui umum; (c) Maklumat berkaitan hendaklah tepat dan lengkap dari semasa ke semasa; dan (d) Menandatangani perakuan pematuhan keselamatan siber yang ditetapkan oleh Kerajaan atau peraturan yang setara / berkaitan yang berkuat kuasa.	Pihak Ketiga
0203 Keselamatan Maklumat Dalam Pengurusan Projek	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; (b) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenai pasti kawalan-kawalan yang diperlukan; dan (c) pengurusan projek hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS AADK.	Semua Pengguna

0204 Peranti Mudah Alih dan Telekerja	
020401 Peranti Mudah Alih	
Dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih hendaklah diberikan perhatian berdasarkan pematuhan kepada perkara – perkara berikut: (a) pendaftaran ke atas peralatan mudah alih; (b) keperluan ke atas perlindungan secara fizikal; (c) mematuhi kawalan ke atas pemasangan perisian peralatan mudah alih; (d) mematuhi kawalan ke atas versi dan patches perisian; dan (e) peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	Semua Pengguna
020402 Telekerja	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua Pengguna

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 03

KESELAMATAN SUMBER MANUSIA

BIDANG 03: KESELAMATAN SUMBER MANUSIA

0301 Sebelum Perkhidmatan

Objektif:

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

030101 Tapisan Keselamatan

Perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; dan (b) Memastikan pelaksanaan tapisan keselamatan melalui Sistem *e-Vetting* untuk warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan.	Semua Pengguna

030102 Terma dan Syarat Perkhidmatan

Persetujuan berkontrak dengan warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: (a) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna

0302 Dalam Perkhidmatan

Objektif:

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

030201 Tanggungjawab Pengurusan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Memastikan pegawai dan kakitangan AADK serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh AADK; dan (b) Memastikan adanya proses tindakan disiplin dan / atau undang-undang ke atas warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku perlanggaran dasar dengan perundangan dan peraturan ditetapkan Agensi; dan	Semua Pengguna

030202 Program Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat

Setiap pengguna perlu diberikan kesedaran, latihan atau kursus mengenai keselamatan aset ICT yang bersesuaian dengan peranan dan tanggungjawab masing-masing secara berterusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan latihan kesedaran mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT AADK secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan	Semua Pengguna

(b) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	
0303 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut : (a) Memastikan semua aset ICT dikembalikan kepada AADK 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 oleh AADK dan / atau terma perkhidmatan.	Semua Pengguna

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 04

PENGURUSAN ASET

BIDANG 04: PENGURUSAN ASET

0401 Tanggungjawab Terhadap Aset

Objektif :

Untuk mengenal pasti aset bagi memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT AADK.

040101 Inventori Aset ICT

Tanggungjawab yang perlu dipatuhi untuk memastikan semua aset ICT dikawal dan dilindungi: (a) Memastikan semua aset ICT dikenal pasti, dikelas, didokumen, diselenggara dan dilupuskan apabila tiba masanya. Maklumat aset direkod dan dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di AADK; dan (d) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pegawai Aset dan Pengguna

040102 Pemulangan Aset ICT

Warga AADK hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan, penamatan perkhidmatan atau penamatan kontrak.	Pegawai Aset dan Pengguna

0402 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.	Semua Pengguna

0403 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut: (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) Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.	Semua Pengguna

0404 Pengurusan Media
Objektif : Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

040401 Pengurusan Media Mudah Alih	
Prosedur pengurusan media mudah alih 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; dan	Semua Pengguna
040402 Pelupusan Media	
Prosedur pelupusan media yang perlu dipatuhi adalah seperti berikut (a) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua Pengguna

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 05

KAWALAN CAPAIAN

BIDANG 05: KAWALAN CAPAIAN

0501 Dasar Kawalan Capaian

Objektif:

Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

050101 Keperluan Kawalan Capaian

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. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan maklumat. Perkara-perkara yang perlu dipastikan termasuk seperti berikut : (a) Kawalan capaian ke atas maklumat dan proses perkhidmatan mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Kawalan capaian ke atas perkhidmatan yang menggunakan kemudahan atau peralatan mudah alih; dan (d) Semakan hak capaian secara berkala dan pembatalan hak capaian.	Pentadbir Sistem ICT

050102 Kawalan Capaian Rangkaian dan Perkhidmatan Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian AADK, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan	Pentadbir Rangkaian ICT

(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	

0502 Pengurusan Capaian Pengguna

Objektif:

Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. la perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

050201 Pendaftaran Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh AADK sahaja boleh digunakan; (b) Akaun pengguna mestilah unik; (c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Pentadbir Sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan AADK. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Akaun pengguna yang baru diwujudkan perlu diberikan kata laluan sementara dan pengguna perlu menukar kata laluan yang kukuh ketika log masuk kali pertama.	Semua Pengguna dan Pentadbir Sistem ICT

050202 Peruntukan Capaian Pengguna	
Proses penyediaan kebenaran capaian pengguna dan pembatalan capaian pengguna ke atas semua aplikasi dan perkhidmatan ICT perlu dipantau berdasarkan keperluan aliran proses sistem.	Pentadbir Sistem ICT
050203 Kajian Semula Hak Capaian Pengguna	
Hak capaian pengguna hendaklah disemak semula pada sela masa yang ditetapkan. Pentadbir Sistem ICT perlu memastikan prosedur semakan ke atas hak capaian pengguna dilaksanakan pada sela masa yang ditetapkan.	Pentadbir Sistem ICT
050204 Pembatalan atau Pengemaskinian Capaian Pengguna	
Pentadbir Sistem ICT boleh membeku atau menamatkan akaun pengguna yang tidak aktif melebihi 90 hari atau apabila dimaklumkan mengenai pegawai yang bersara, bertukar atau berlaku perubahan dalam bidang tugas. Jika perlu, Pentadbir Sistem ICT boleh membekukan akaun pengguna yang bercuti atau berkursus panjang.	Pentadbir Sistem ICT
0503 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
050301 Sekatan Akses Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pentadbir Sistem ICT

050302 Prosedur Log Masuk yang Selamat	
Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan / prosedur yang berkuat kuasa; (b) Menjana amaran *(alert)* sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; (c) Mengawal capaian ke atas sistem dan aplikasi menggunakan prosedur log masuk yang terjamin; (d) Mewujudkan satu pengenalan diri *(ID)* yang unik untuk setiap penguna; dan (e) Mewujudkan jejak audit ke atas semua capaian sistem dan aplikasi.	Pentadbir Sistem ICT
050303 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh AADK seperti berikut: (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 aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	Semua Pengguna dan Pentadbir Sistem ICT

(g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan (i) Tentukan had masa pengesahan maksima adalah sepuluh (10) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan.	
050304 Kawalan Akses kepada Kod Sumber Program	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh Pemilik Sistem dan Pentadbir Sistem ICT. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Akses kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; (b) Kod sumber *(source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik AADK. (c) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; dan (d) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan.	Pemilik Sistem, Pihak Ketiga dan Pentadbir Sistem ICT

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 06

KRIPTOGRAFI

BIDANG 06: KRIPTOGRAFI

0601 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui pelaksanaan kriptografi yang berkesan.

060101 Enkripsi

Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah mempunyai fungsi enkripsi *(encryption).*	Pentadbir Sistem ICT

060102 Tandatangan Digital

Penggunaan tandatangan digital adalah digalakkan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat terperingkat secara elektronik.	Semua Pengguna

0602 Pengurusan Prasarana Kekunci Awam (PKI)

Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Penggunaan PKI perlu mematuhi perkara-perkara seperti berikut: (a) PKI token hendaklah digunakan bagi capaian dan tandatangan digital ke atas sistem yang dikhususkan sahaja mengikut peranan atau tahap kelayakan;	Semua Pengguna

(b) PKI token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian PKI token untuk sebarang capaian dan tandatangan digital sistem adalah tidak dibenarkan sama sekali; dan (d) Sebarang kehilangan, kerosakan dan kata laluan yang disekat perlu dimaklumkan kepada pegawai yang diberi kuasa.	

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 07

KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Kawasan Selamat

Objektif :

Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat AADK.

070101 Perimeter Keselamatan Fizikal

Bertujuan untuk menghalang akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat AADK. 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) Memasang alat penggera atau kamera litar tertutup; (c) Mengehadkan jalan keluar masuk; (d) Mewujudkan perkhidmatan kawalan keselamatan; (e) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (f) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan mengikut Arahan Keselamatan Kerajaan; (g) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; dan (h) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Jabatan, *CIO*, *ICTSO* serta Pentadbir Pusat Data dan Rangkaian

070102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Pas Pekerja hendaklah dijaga dengan baik sepanjang berkhidmat di AADK; (b) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama premis-premis AADK. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (c) Kehilangan pas mestilah dilaporkan dengan segera.	Semua Pengguna
070103 Keselamatan Pejabat, Bilik dan Kemudahan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi keselamatan pejabat, bilik dan kemudahan. Kawasan larangan di AADK adalah seperti berikut: (a) Bilik Ketua Pengarah; (b) Bilik Timbalan Ketua Pengarah (Pengurusan), (c) Bilik Timbalan Ketua Pengarah (Operasi); (d) Bilik semua Pengarah Bahagian; (e) Pusat Data *(Data Centre)* dan (f) Kawasan-kawasan lain yang dikategorikan sebagai Kawasan Larangan oleh AADK. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Akses kepada kawasan larangan hanyalah kepada pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua Pengguna

070104 Perlindungan daripada Ancaman Luar dan Persekitaran	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. AADK perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pegawai Keselamatan Jabatan
070105 Bekerja di Kawasan Selamat	
Kawasan larangan di AADK mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: (a) Pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Pemantauan dibuat menggunakan sistem kamera litar tertutup atau lain-lain peralatan yang sesuai; (d) Peralatan keselamatan perlu diperiksa secara berjadual; (e) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; (f) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan; dan (g) Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT.	Semua Pengguna

070106 Kawasan Penyerahan dan Pemunggahan	
Kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. AADK hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat Iain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Semua Pengguna

0702 Keselamatan Peralatan ICT
Objektif: Melindungi peralatan ICT AADK dari kehilangan, kerosakan, kecurian serta penyalahgunaan kepada peralatan tersebut.

070201 Penempatan dan Perlindungan Peralatan ICT	
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi termasuk: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (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 BTMK;	Semua Pengguna

(e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

(f) Pengguna mesti memastikan perisian antivirus di komputer mereka sentiasa aktif *(activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

(g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply (UPS)*;

(i) Semua peralatan ICT hendaklah disimpan atau diletakkan ditempat 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;

(j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;

(k) Peralatan ICT yang hendak dibawa keluar dari premis AADK untuk tujuan penyelenggaraan perlu mendapat kelulusan BTMK dan direkodkan bagi tujuan pemantauan;

(l) Peralatan ICT yang hilang hendaklah dilaporkan kepada *ICTSO* dan Pegawai Aset dengan segera;

(m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran BTMK;

(o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan dalam Sistem Pengurusan Aduan ICT untuk dibaikpulih;

(p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(q) Konfigurasi alamat *IP* tidak dibenarkan diubah daripada alamat *IP* yang asal;

(r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir *(administrator password)* yang telah ditetapkan oleh BTMK; (s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (t) Pengguna hendaklah memastikan semua perkakasan komputer,pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; dan (u) Memastikan *plug* dicabut daripada suis utama *(main switch)* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
070202 Utiliti Sokongan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melindungi peralatan ICT daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. (b) Semua kemudahan sistem seperti penghawa dingin, bekalan air, kumbahan dan pengalihan udara perlu dilindungi dari kegagalan bekalan elektrik dan sebarang gangguan; dan (c) Kemudahan sistem perlu diperiksa dan diuji agar sentiasa berfungsi dengan baik bagi mengurangkan risiko kegagalan;	Semua Pengguna dan Pegawai Keselamatan Jabatan
070203 Keselamatan Kabel	
Kabel kuasa dan telekomunikasi yang menyokong perkhidmatan keselamatan maklumat hendaklah dilindungi bagi mengelakkan kerosakan, pintasan atau gangguan perkhidmatan.	Pentadbir Rangkaian ICT

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (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.	
070204 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset serta Unit Teknikal dan Helpdesk

070205 Pergerakan Aset	
Perkakasan yang dibawa keluar dari premis AADK adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapatkan kelulusan mengikut peraturan dibawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan AADK bagi membawa keluar perkakasan atau maklumat tertakluk kepada tujuan yang dibenarkan; dan (b) Memastikan aktiviti pinjaman dan pemulangan perkakasan ICT direkodkan.	Pengguna dan Pegawai Aset
070206 Keselamatan Peralatan ICT di Luar Premis	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis AADK. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Semua Pengguna
070207 Pelupusan Perkakasan	
Pelupusan perkakasan ICT melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh AADK dan ditempatkan di AADK. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan AADK.	Semua Pengguna dan Pegawai Aset

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Semua kandungan peralatan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

(b) Data-data dalam storan bagi peralatan ICT yang akan dilupuskan hendaklah dihapuskan dengan cara yang selamat;

(c) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

(d) Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan dan mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

(e) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem;

(f) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

(g) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.

ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

iii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di AADK;

iv. Memindah keluar dari premis AADK mana-mana peralatan ICT yang hendak dilupuskan tanpa kebenaran; dan

v. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Unit Pengurusan Aset, AADK.

(h) Pengguna bertanggungjawab memastikan segala maklumat penting di dalam komputer disalin pada media storan kedua seperti pemacu kedua

sebelum maklumat tersebut dihapuskan daripada peralatan komputer yang hendak dilupuskan; dan (i) Maklumat lanjut berhubung pelupusan boleh dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan yang berkuat kuasa.	
070208 Kawalan Perkakasan	
Pengguna perlu memastikan bahawa peralatan ICT dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: (a) Tamatkan sesi aktif apabila selesai tugasan kerja jarak jauh; (b) *Log-off* komputer meja dan komputer riba apabila selesai bertugas; dan (c) Memastikan komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Semua Pengguna
070209 Polisi *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* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faks dan mesin fotostat.	Semua Pengguna

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 08

KESELAMATAN OPERASI

BIDANG 08: KESELAMATAN OPERASI

0801 Pengurusan Pengendalian Prosedur

Objektif :

Untuk memastikan kemudahan pemprosesan maklumat adalah berfungsi dengan baik dan selamat dari sebarang ancaman atau gangguan.

080101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur keselamatan siber yang diwujud, dikenalpasti dan digunapakai hendaklah didokumen disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua Pengguna

080102 Pengurusan Perubahan

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Semua Pengguna

(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.	
080103 Pengurusan Kapasiti	
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. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT
080104 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*; (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan (c) Data yang mengandungi maklumat terperingkat tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Pentadbir Sistem ICT

0802 Perlindungan daripada Perisian Hasad

Objektif:

Melindungi integriti perisian dan kemudahan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian hasad seperti *virus*, *malware* dan sebagainya.

080201 Kawalan daripada Perisian Hasad

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada perisian hasad hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang mesti dipatuhi termasuk yang berikut : (a) Memasang sistem keselamatan untuk mengesan perisian hasad seperti antivirus, *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 mana-mana undang-undang bertulis yang berkuatkuasa; (c) Mengimbas semua perisian atau sistem dengan *antivirus* sebelum menggunakannya; (d) Mengemaskini 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 hasad dan cara mengendalikannya; dan (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.	Pentadbir Sistem ICT

0803 Penduaan (*Backup*)

Objektif:

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa dan memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.

080301 Penduaan Maklumat *(Information Backup)*

Salinan penduaan maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur penduaan yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan 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. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan (d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan.	Pentadbir Sistem ICT

0804 Log dan Pemantauan

Objektif:

Memastikan pengesanann aktiviti pemprosesan maklumat yang tidak dibenarkan.

080401 Log Sistem	
Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan / pekeliling terkini yang dikeluarkan oleh Kerajaan serta dikawal bagi mengekalkan integriti data. Pentadbir Sistem ICT 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 ICT hendaklah melaporkan kepada *CERT* AADK.	Pentadbir Sistem ICT
080402 Perlindungan Maklumat Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;	Pentadbir Sistem ICT
080403 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala;	Pentadbir Sistem ICT

(c) Aktiviti pentadbiran dan pengendali sistem perlu direkodkan; dan (d) Kesalahan, kesilapan dan / atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya.	
080404 Penyegerakan Jam	
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam AADK atau domain keselamatan perlu diselaraskan ke Pelayan *NTP (Network Time Protocol).*	Pentadbir Pusat Data dan Rangkaian
0805 Kawalan Perisian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem pengoperasian.	
080501 Perisian pada Sistem Pengoperasian	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem pengoperasian. Langkah-langkah yang perlu dipatuhi seperti berikut: (a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; (b) Aplikasi dan sistem pengoperasian hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku; dan (c) Setiap konfigurasi keatas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	Pentadbir Sistem ICT

0806 Kawalan Kerentanan Teknikal

Objektif:

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

080601 Kawalan dari Ancaman Teknikal

Kawalan kerentanan teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan ujian penembusan bagi memperoleh maklumat kerentanan teknikal ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenalpasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk penguraian risiko berkaitan.	Pentadbir Sistem ICT

080602 Sekatan ke atas Pemasangan Perisian

Garis panduan atau prosedur bagi mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Garis panduan atau prosedur yang jelas berkaitan jenis perisian yang dibenarkan dan tidak dibenarkan (seperti perisian untuk kegunaan peribadi) perlu dipatuhi; dan (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa.	Unit Teknikal dan Helpdesk

0807 Audit Sistem Maklumat	
Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.	
080701 Kawalan Audit Sistem Maklumat	
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas sistem ICT.	*ICTSO*

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 09

KESELAMATAN KOMUNIKASI

BIDANG 09: KESELAMATAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian

Objektif:

Melindungi keselamatan maklumat dalam rangkaian dan infrastruktur sokongan.

090101 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggunjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *User Acceptance Test (UAT)* semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan AADK; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran *ICTSO*; (h) Memasang perisian *Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat AADK; (i) Memasang *content filtering* pada *internet gateway* untuk menyekat aktiviti yang dilarang;	Pentadbir Pusat Data dan Rangkaian

(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan AADK adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian AADK sahaja dan penggunaan modem adalah dilarang sama sekali; (l) Kemudahan bagi *wireless LAN* hendaklah dipantau dan dikawal penggunaannya; dan (m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance (SLA)* yang telah ditetapkan.	
090102 Keselamatan Perkhidmatan Rangkaian	
Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah: Mekanisme keselamatan, tahap kesediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman ataupun menggunakan sumber luar; Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan AADK; dan Sebarang aktiviti yang dilarang seperti yang termaktub di dalam undang-undang yang berkuat kuasa perlu disekat melalui penggunaan *content filtering*.	Pentadbir Pusat Data dan Rangkaian
090103 Pengasingan Rangkaian	
Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara–perkara yang perlu dipatuhi adalah: (a) Mengenal pasti fungsi dan tanggungjawab pengguna;	Pentadbir Pusat Data dan Rangkaian

(b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan (e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	
0902 Pemindahan Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara AADK dan agensi luar terjamin.	
090201 Prosedur Pemindahan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pemindahan maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pemindahan maklumat dan perisian di antara AADK dengan agensi luar; dan (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari AADK.	Pentadbir Sistem ICT

090202 Perjanjian Pemindahan Maklumat	
AADK perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara MAMPU dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: (a) Mengawal penghantaran dan penerimaan maklumat antara AADK dengan agensi luar; dan (b) Memastikan kerahsiaan, integriti dan ketersediaan maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara AADK dengan agensi luar.	Pentadbir Sistem ICT
0903 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di AADK hendaklah dipantau secara berterusan oleh Pentadbir E-mel bagi memenuhi keperluan etika penggunaan e-mel dan internet yang terkandung dalam mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh AADK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh AADK; (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 hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;	Semua Pengguna

(g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti 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) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (k) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti *yahoo.com, gmail.com, streamyx.com.my* dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; (l) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; dan (m) Tempoh penyimpanan e-mel di dalam server e-mel adalah dihadkan kepada tiga puluh (30) hari selepas seseorang kakitangan bertukar ke agensi lain atau menamatkan perkhidmatan.	
0904 Perjanjian Kerahsiaan	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut : (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua Pengguna

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keperluan Keselamatan Sistem Maklumat

Objektif:

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

100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambilkira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem *output* untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan *(validation)* untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem dan Pentadbir Sistem ICT

100102 Keselamatan Sistem / Aplikasi dalam Rangkaian Awam	
Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi AADK. Contoh perkhidmatan sumber luaran ialah: i. Perisian Sebagai Satu Perkhidmatan; ii. Platform Sebagai Satu Perkhidmatan; iii. Infrastruktur Sebagai Satu Perkhidmatan; iv. Storan Pengkomputeran Awan; dan v. Pemantauan Keselamatan. (b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; dan (c) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem ICT
100103 Melindungi Transaksi Perkhidmatan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian transaksi perkhidmatan aplikasi hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; dan (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.	Pemilik Sistem dan Pentadbir Sistem ICT

1002 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

100201 Polisi Keselamatan dalam Pembangunan Sistem

Tatacara pembangunan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi semasa proses pembangunan sistem.	Pentadbir Sistem ICT

100202 Prosedur Kawalan Perubahan Sistem

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan sistem yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (c) Mengawal perubahan dan / atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; dan (d) Capaian kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	Pemilik Sistem dan Pentadbir Sistem ICT

100203 Semakan Teknikal Aplikasi Selepas Perubahan Platform	
Semakan dan pengujian terhadap aplikasi kritikal perlu dilaksanakan sekiranya berlaku perubahan terhadap platform pengoperasian bagi memastikan fungsi dan operasi sistem tidak terjejas. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan sistem aplikasi, integriti data dan kawalan akses disemak supaya operasi sistem tidak terjejas apabila perubahan platform dilaksanakan; dan (b) Ujian penerimaan pengguna perlu dilaksanakan setelah perubahan platform selesai dilaksanakan.	Pentadbir Sistem ICT
100204 Kawalan Terhadap Perubahan Kepada Perisian	
Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	Pentadbir Sistem ICT
100205 Prinsip Kejuruteraan Sistem Yang Selamat	
Prinsip kejuruteraan keselamatan sistem hendaklah dibangunkan, didokumenkan, dikaji dan digunapakai ke atas semua pelaksanaan sistem maklumat.	Pentadbir Sistem ICT
100206 Persekitaran Pembangunan Selamat	
Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem. Secara umumnya kitar hayat pembangunan sistem termasuk skop dan objektif sistem, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pemasangan, konfigurasi, penyelenggaraan dan pelupusan.	Pentadbir Sistem ICT

100207 Pembangunan Sistem Secara Luaran	
Sebarang aktiviti pembangunan sistem yang melibatkan sumber luar perlu dikawal selia dan dipantau. Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: (a) Memastikan spesifikasi perolehan mengandungi klausa tertentu berhubung keperluan keselamatan, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi Pasukan Pembangunan; (b) Organisasi hendaklah memastikan *Intellectual Property Rights (IPR)* dan kod sumber menjadi hak milik organisasi; dan (c) Memasukkan klausa ke dalam kontrak yang membenarkan AADK melaksanakan semakan terhadap kod sumber.	Pentadbir Sistem ICT
100208 Ujian Keselamatan Sistem	
Aktiviti pengujian penerimaan sistem hendaklah dilaksanakan ke atas sistem baru, naik taraf dan versi baru berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integriti data, pengujian hendaklah dijalankan ke atas tiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data *(input),* peringkat pemprosesan data *(process)* dan peringkat penjanaan laporan *(output).*	Pentadbir Sistem ICT
100209 Ujian Penerimaan Sistem	
Semua sistem baharu (termasuklah sistem yang dikemaskini / diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT

1003 Data Ujian	
Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.	
100301 Perlindungan Data Ujian	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; dan (b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian.	Pentadbir Sistem ICT

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 11

HUBUNGAN PEMBEKAL

BIDANG 11: HUBUNGAN PEMBEKAL

1101 Keselamatan Maklumat Dalam Hubungan Pembekal

Objektif:

Memastikan perkhidmatan yang ditawarkan oleh pembekal mempunyai tahap keselamatan ICT yang bersesuaian.

110101 Polisi Keselamatan Maklumat ke atas Pembekal

Semua pembekal adalah tertakluk kepada PKS AADK yang berkuat kuasa. Perkara - perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembekal hendaklah menandatangani Surat Akuan Pematuhan PKS AADK; (b) Pembekal hendaklah menandatangani Akuan Akta Rahsia Rasmi 1972; (c) Pembekal hendaklah menjalani ujian tapisan keselamatan melalui sistem e-vetting tertakluk kepada prosedur yang berkuat kuasa; (d) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas; (e) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa; dan (f) Menyediakan pelan kontigensi *(contingency plan)* bagi memastikan ketersediaan kemudahan pemprosesan maklumat.	Pembekal dan *ICTSO*

110102 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal	
Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui oleh setiap pembekal yang diberikan kebenaran mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk AADK. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada AADK selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.	Pembekal dan *ICTSO*
110103 Rantaian Maklumat Pembekal	
Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal Iain yang memberikan perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pembekal dan Pentadbir Sistem ICT
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.	

110201 Pemantauan dan Penilaian Perkhidmatan Pembekal	
Agensi hendaklah memantau, menyemak dan mengaudit perkhidmatan pembekal perkhidmatan ICT secara berkala.	Pentadbir Sistem ICT
110202 Pengurusan Perubahan Melibatkan Perkhidmatan Pembekal	
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut prosedur yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Perubahan di dalam perjanjian bersama pembekal; (b) Perubahan yang dilakukan oleh agensi bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pentadbir Sistem ICT dan Pembekal

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

BIDANG 12: PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

1201 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

Objektif :

Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat bagi menjamin sistem penyampaian perkhidmatan yang berkesan.

120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan insiden keselamatan maklumat hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	*ICTSO* dan *CERT* AADK

120102 Pelaporan Insiden Keselamatan Maklumat	
Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan kepada *ICTSO* dan *CERT* AADK dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki digunakan; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka.	Semua Pengguna

120103 Pelaporan Kelemahan Keselamatan Maklumat	
Warga AADK dan pembekal yang menggunakan sistem dan perkhidmatan maklumat AADK dikehendaki melaporkan sebarang kelemahan keselamatan maklumat ICT.	Semua Pengguna
120104 Penilaian dan Keputusan Insiden Keselamatan Maklumat	
Insiden keselamatan ICT perlu dinilai dan keputusan perlu dibuat jika pasti insiden tersebut boleh diklasifikasikan sebagai insiden keselamatan maklumat. (a) Penilaian perlu dibuat berasaskan skim klasifikasi insiden yang dipersetujui; (b) Insiden perlu disusun mengikut kepentingan dan implikasi kepada AADK; dan (c) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan.	*CERT* AADK
120105 Tindak Balas Terhadap Insiden Keselamatan Maklumat	
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosedur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan maklumat adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah pemulihan. Kawalan-kawalan yang perlu diambilkira di dalam pengumpulan maklumat dan pengurusan pengendalian insiden keselamatan maklumat adalah seperti berikut: (a) Mengumpul bahan bukti secepat yang mungkin selepas kejadian; (b) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu; (c) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya;	*CERT* AADK

(d) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku.	
120106 Pembelajaran daripada Insiden Keselamatan Maklumat	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	*CERT* AADK
120107 Pengumpulan dan Pengendalian Bukti	
Pelaporan insiden keselamatan maklumat digunakan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Selain itu, ia juga digunakan bagi mengenalpasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada AADK. Kawalan-kawalan yang perlu diambilkira di dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyediakan pelan kontingensi serta tindakan pemulihan segera; dan (c) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	*CERT* AADK

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 13

KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BIDANG 13: KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Dasar Kesinambungan Perkhidmatan

Objektif :

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

130101 Perancangan Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana ICT *(DRP)*

PKP adalah di bawah tanggungjawab Bahagian Khidmat Pengurusan (BKP) dan *DRP* merupakan salah satu daripada komponen PKP di bawah seliaan BTMK. PKP dan *DRP* hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab Pasukan Pemulihan Bencana; (b) Melaksanakan prosedur-prosedur pemulihan dalam jangka masa yang ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) Mengadakan program latihan / simulasi kepada pengguna mengenai prosedur pemulihan bencana sekurang-kurangnya setahun sekali; dan (e) Mewujudkan Pusat Pemulihan Bencana di lokasi lain.	*CIO* / Koordinator PKP

130102 Ketersediaan Fasiliti Pemprosesan Maklumat	
Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat di tahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi / platform pemprosesan) perlu diwujudkan. Untuk tujuan itu, perkara berikut wajar diberi tumpuan: (a) AADK perlu mengenalpasti keperluan kebolehsediaan sistem maklumat (memahami sejauh mana kritikalnya kebolehsediaan sesuatu sistem maklumat); (b) Jika kebolehsediaan sistem maklumat tidak dapat dipastikan dengan satu lokasi pemprosesan, maka fasiliti pemprosesan bertindan perlu dipertimbangkan; (c) Fasiliti pemprosesan bertindan perlu diuji bagi memastikan kesiapsediaan menjalankan operasi apabila pemprosesan utama gagal berfungsi; dan (d) Kewujudan pemprosesan bertindan boleh membawa risiko kepada kewibawaan dan kerahsiaan maklumat dan sistem maklumat. Hal ini perlu diambilkira semasa sesuatu sistem maklumat itu direkabentuk.	*CIO* / Koordinator PKP

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

BIDANG 14

PEMATUHAN

BIDANG 14: PEMATUHAN

1401 Pematuhan dan Keperluan Perundangan

Objektif :

Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran undang-undang dan peraturan berkaitan dengan keselamatan maklumat yang sedang berkuat kuasa.

140101 Keperluan Perundangan

Setiap pengguna di AADK hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber AADK dan undang-undang atau peraturan-peraturan lain yang berkaitan yang telah berkuat kuasa. Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di AADK adalah seperti di **Lampiran 2**.	Semua Pengguna

140102 Hak Harta Intelek

Kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelek perlu dipatuhi. Pihak yang terlibat dengan pengurusan keselamatan maklumat di AADK perlu melaksanakan kawalan terhadap keperluan perlesenan supaya hanya perisian yang mempunyai lesen yang sah digunakan.	Semua Pengguna

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 yang berkuat kuasa.	Semua Pengguna

140104 Perlindungan Maklumat Peribadi dan Privasi Pengguna	
Perlindungan maklumat peribadi dan privasi pengguna adalah dijamin seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkaitan.	Semua Pengguna
140105 Pelanggaran Perundangan	
Pelanggaran Polisi Keselamatan Siber AADK boleh dikenakan tindakan tatatertib.	Semua Pengguna
1402 Kajian Semula Keselamatan Maklumat	
Objektif : Memantapkan pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.	
140201 Keperluan Audit	
Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua Pengguna
140202 Pematuhan Polisi Keselamatan Maklumat	
Pelaksanaan projek yang berkaitan dengan keselamatan maklumat di AADK perlu mematuhi prosedur dan garis panduan yang ditetapkan serta peraturan yang digariskan dalam PKS AADK dalam setiap aktiviti pengurusan projek.	Semua Pengguna

Semua pihak yang terlibat dalam sesuatu projek perlu dimaklumkan berkenaan arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian (seperti Akta Rahsia Rasmi).	
140203 Kajian Semula Pematuhan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan siber di AADK.	*ICTSO*

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

TERMA DAN TAKRIFAN

TERMA DAN TAKRIFAN

(a) **Risiko**

Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.

(b) **Penilaian Risiko**

Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.

(c) ***Antivirus***

Perisian yang mengimbas dan memusnahkan sebarang kemungkinan serangan virus pada media storan seperti cakera padat, pita magnetik dan pita optik.

(d) **Ancaman**

Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.

(e) ***Backup* (sandaran)**

Proses penduaan sesuatu dokumen atau maklumat.

(f) **Aset ICT**

Bermaksud semua yang mempunyai nilai kepada organisasi merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

(g) ***Clear Desk***

Bermaksud tidak meninggalkan sebarang dokumen yang sensitif di atas meja.

(h) ***Clear Screen***

Bermaksud tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.

(i) ***Mobile Code***

Bermaksud kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.

(j) **Kriptografi**

Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

(k) **Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK)**

KPKK juga dikenali sebagai *Chief Government Security Office (CGSO)*. Pejabat ini di bawah Jabatan Perdana Menteri yang menyedia dan mengeluarkan peraturan keselamatan perlindungan serta memberi khidmat nasihat keselamatan perlindungan dari aspek fizikal, dokumen, personel, dan keselamatan ICT.

(l) ***Computer Emergency Response Team (CERT)***

Bermaksud Pasukan Tindak Balas Insiden Keselamatan ICT. *CERT* AADK yang dilantik akan berhubung terus dengan pasukan *CERT* Kementerian Dalam Negeri (KDN) yang bertindak sebagai *first level support* kepada *NACSA* dalam mengendali insiden keselamatan ICT.

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

LAMPIRAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER

AGENSI ANTIDADAH KEBANGSAAN

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan / Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber AADK; dan

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

.....

(Tandatangan Pegawai)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT *(ICTSO)* AADK

.....

(Tandatangan dan Cop Jawatan)

Tarikh : .....

LAMPIRAN 2

SENARAI PERUNDANGAN DAN PERATURAN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
1.	Akta Rahsia Rasmi 1972	KPKK
2.	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi *(*ICT*)* bertarikh 4 April 2001.	MAMPU
3.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi Kerajaan bertarikh 28 November 2003.	MAMPU
4.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 - Tatacara Pengurusan Aset Alih Kerajaan bertarikh 2 Mac 2007.	Kementerian Kewangan Malaysia
5.	Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi *(*ICT*)* Sektor Awam bertarikh 9 November 2006.	MAMPU
6.	Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.	MAMPU
7.	Pekeliling Perbendaharaan Malaysia - Tatacara Pengurusan Aset Alih Kerajaan : Pelupusan.	Kementerian Kewangan Malaysia
8.	Akta 629 - Akta Arkib Negara 2003.	Arkib Negara Malaysia
9.	Arahan Keselamatan	KPKK
10.	Arahan Teknologi Maklumat 2007 bertarikh 19 Disember 2007.	MAMPU
11.	Arahan Amalan 2013 (Jadual Pelupusan Rekod Fungsian)	Arkib Negara Malaysia
12.	Pekeliling Perkhidmatan Bil. 5 Tahun 2007: Panduan Pengurusan Pejabat bertarikh 30 April 2007	JPA

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
13.	Surat Pekeliling Am Bil. 1 Tahun 1997: Peraturan Pemeliharaan Rekod-rekod Kerajaan bertarikh 11 April 1997.	Arkib Negara Malaysia
14.	Pekeliling Am Bil 3 Tahun 2009: Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 17 November 2009.	MAMPU
15.	Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000.	MAMPU
16.	Akta Hak Cipta (Pindaan) 2012 bertarikh 1 Mac 2012.	KPDNHEP
17.	Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team (GCERT)* oleh *NACSA* bertarikh 28 Januari 2019.	NACSA
18.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0.	MAMPU