



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

VERSI 5.0

TERBUKA

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

I. KELULUSAN DOKUMEN

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
		
Nama : Salasiah binti Abdullah	Nama : Lilian Lou Yang Cheng	Nama : Chan Hong Jin
Jawatan : Penolong Pengarah (PP(TM)4), Bahagian Teknologi Maklumat & Komunikasi	Jawatan : Pengarah Bahagian Teknologi Maklumat & Komunikasi (PTM)	Jawatan : Timbalan Ketua Pengarah (Pengurusan) (TKP(P)), Agensi Antidadah Kebangsaan
Tarikh : 1 April 2021	Tarikh : 1 April 2021	Tarikh : 1 April 2021

II. REKOD PINDAAN DOKUMEN

TARIKH	VERSI	BAB/MUKA SURAT	BUTIRAN PINDAAN
Dis 2009	1.0		Dokumen Asal
Jun 2013	2.0		Penambahbaikan Dasar Keselamatan ICT AADK
18 Feb 2016	3.0	19	Kemaskini pada perkara 0101: Pelaksanaan Dasar
		22	Kemaskini pada perkara 0201: Infrastruktur Organisasi dengan mengeluarkan tanggungjawab Pengurus ICT
		28	Kemaskini pada perkara 020111 (Pindaan Jawatankuasa Keselamatan (JKICT) kepada Mesyuarat Jawatankuasa Keselamatan ICT AADK (JICTA))
		30, 31, 32, 81, 84, 85 dan 89	Penambahan pada perkara 020202, 020203, 020204, 080502, 090202, 090203 dan 100102
		57	Kemaskini pada perkara 050207: Pelupusan Perkakasan (f)

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	2 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

		58	Kemaskini pada perkara 060501: Penduaan (Backup) (c)
		69	Kemaskini pada perkara 070203: Pengurusan Kata Laluan (c)
31 Mac 2016	3.1	1	Melabelkan DKICT sebagai dokumen 'Terbuka'
		17	Kemaskini pada perkara G. Pindaan dan Kemaskini dengan penambahan pernyataan 'Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun' bagi memenuhi keperluan pada perkara 0103 Penyelenggaraan Dasar
		31	Kemaskini pada perkara 020202 Keselamatan Maklumat Dalam Pengurusan Projek (h)
		51	Kemaskini pada perkara 050401 Dokumen pada DKICT dengan penambahan pernyataan 'pengekaln'.
		69	Kemaskini pada perkara 070201: Akaun Pengguna (f)
		96	Kemaskini pada Lampiran 1: Surat Akaun Pematuhan DKICT AADK
		97, 101	Penambahan pada Lampiran 2: Proses Kerja Pelaporan Insiden Keselamatan ICT MAMPU dan Lampiran 3: Senarai Perundangan dan Peraturan.
18 Mei 2017	4.0		Penambahbaikan Dasar Keselamatan ICT AADK versi 3.1
4 April 2018	4.1	68	Kemaskini nama pegawai Penyedia dan Pelulus di muka hadapan Dokumen ISMS. Kemaskini pada perkara 070203: Pengurusan Kata Laluan (c)

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	3 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

1 April 2021	5.0	1	Kemaskini nama pegawai Penyedia dan Pelulus di muka hadapan Dokumen ISMS.
		24	Kemaskini perkara 020103 Pegawai Keselamatan ICT (ICTSO).
		24	Penambahan perkara 020104 Pengurus ICT.
		27	Kemaskini perkara 020111 Jawatankuasa Pemandu ICT AADK (JICTA).
		28	Penambahan perkara 020110 Pemilik Sistem.
		30	Kemaskini perkara 020301 Keperluan Keselamatan Kontrak dengan Pihak Ketiga.
		57	Kemaskini perkara 060302 Penerimaan Sistem.
		76	Pembatalan perkara 070402 Kad Pintar.
		76	Penambahan perkara 070402 Prasarana Kekunci Awam (PKI).
		99	Kemaskini perkara 12 Glosari dengan pertambahan terma Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK) dan CERT.
		101	Kemaskini pada Lampiran 1 Surat Akuan Pematuhan Dasar Keselamatan ICT AADK.
		102	Kemaskini pada Lampiran 2: Proses Kerja Pelaporan Insiden Keselamatan ICT AADK melibatkan perubahan portfolio MAMPU kepada NACSA.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	4 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

KANDUNGAN

I. KELULUSAN DOKUMEN.....	2
II. REKOD PINDAAN DOKUMEN.....	2
A. PENGENALAN	10
B. OBJEKTIF.....	10
C. PERNYATAAN DASAR	11
D. SKOP.....	12
E. PRINSIP-PRINSIP.....	14
F. PENILAIAN RISIKO KESELAMATAN ICT	16
G. MAKLUMAT LANJUT.....	16
H. DASAR WAJIB DAN TERPAKAI	17

PERKARA 01 : PELAKSANAAN DAN PENYELENGGARAAN DASAR KESELAMATAN

0101 Pelaksanaan Dasar	19
0102 Pemakaian Dasar	19
0103 Penyebaran Dasar.....	19
0104 Penyelenggaraan Dasar	20

PERKARA 02 : PENGURUSAN KESELAMATAN ICT.....

0201 Infrastruktur Organisasi Dalam	22
020101 Ketua Pengarah Agensi Antidadah Kebangsaan	22
020102 Ketua Pegawai Maklumat (CIO)	22
020103 Pegawai Keselamatan ICT (ICTSO)	23
020104 Pengurus ICT	23
020105 Pentadbir Sistem ICT	24
020106 Pentadbir Rangkaian ICT	24
020107 Pentadbir Sistem Aplikasi	24
020108 Pentadbir Laman Web.....	25
020109 Pentadbir Pusat Data.....	256
020110 Pemilik Sistem.....	256
020111 Jawatankuasa Pemandu ICT AADK (JICTA)	27
0202 Pasukan Tindak Balas Insiden Keselamatan ICT AADK (CERT AADK)	28
0203 Pihak Ketiga	29
020301 Keperluan Keselamatan Melibatkan Kontrak Pihak Ketiga	29
020302 Keselamatan Maklumat Dalam Pengurusan Projek.....	300
020303 Polisi Keselamatan Maklumat Berkaitan Hubungan Pembekal	311

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	5 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

020304 Rangkaian Pembekal ICT	32
 PERKARA 03 : PENGURUSAN ASET	35
0301 Akauntabiliti Aset ICT	35
030101 Inventori Aset ICT	35
0302 Pengelasan Maklumat	36
0303 Pengendalian Maklumat.....	36
 PERKARA 04 : KESELAMATAN SUMBER MANUSIA.....	38
0401 Keselamatan Sumber Manusia.....	38
0402 Sebelum Berkhidmat.....	38
0403 Dalam Perkhidmatan	38
0404 Bertukar Atau Tamat Perkhidmatan.....	39
0405 Program Kesedaran, Pendidikan Dan Latihan Keselamatan ICT	39
 PERKARA 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN	41
0501 Keselamatan Kawasan	41
050101 Kawalan Kawasan.....	41
050102 Kawalan Masuk Fizikal.....	42
050103 Kawasan Larangan	42
0502 Keselamatan Peralatan	43
050201 Peralatan ICT	43
050202 Media Storan	45
050203 Media Tandatangan Digital.....	46
050204 Media Perisian dan Aplikasi.....	46
050205 Penyelenggaraan Perkakasan	46
050206 Peralatan di Luar Premis.....	47
050207 Pelupusan Perkakasan.....	48
0503 Keselamatan Persekitaran	49
050301 Kawalan Persekitaran.....	49
050302 Bekalan Kuasa.....	50
050303 Kabel	51
050304 Prosedur Kecemasan	51
050305 Utiliti.....	51

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	6 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0504 Keselamatan Dokumen	52
050401 Dokumen.....	52
 PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI	 54
0601 Pengurusan Pengendalian Prosedur	54
060101 Pengendalian Prosedur.....	54
060102 Kawalan Perubahan.....	54
060103 Pengasingan Tugas dan Tanggungjawab	55
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	55
060201 Perkhidmatan Penyampaian.....	55
0603 Perancangan Dan Penerimaan Sistem.....	56
060301 Perancangan Kapasiti	56
060302 Penerimaan Sistem.....	56
0604 Perisian Berbahaya.....	57
060401 Perlindungan Perisian Berbahaya.....	57
060402 Perlindungan dari <i>Mobile Code</i>.....	58
0605 <i>Housekeeping</i>.....	58
060501 Penduaan (<i>Backup</i>)	58
0606 Pengurusan Rangkaian	59
060601 Kawalan Infrastruktur Rangkaian	59
0607 Pengurusan Media	60
060701 Penghantaran dan Pemindahan.....	60
060702 Prosedur Pengendalian Media	60
060703 Keselamatan Sistem Dokumentasi.....	61
0608 Pengurusan Pertukaran Maklumat.....	61
060801 Pertukaran Maklumat	61
060802 Pengurusan Mel Elektronik (E-mel)	62
0609 Perkhidmatan e-Dagang (<i>Electronic Commerce Services</i>)	63
060901 E-Dagang	63
060902 Maklumat Umum	64
0610 Pemantauan	64
061001 Pengauditan dan Forensik ICT	64
061002 Jejak Audit.....	65
061003 Sistem Log	66
061004 Pemantauan Log.....	66

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	7 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 07 : KAWALAN CAPAIAN.....	69
0701 Dasar Kawalan Capaian.....	69
070101 Keperluan Kawalan Capaian.....	69
0702 Pengurusan Capaian Pengguna	69
070201 Akaun Pengguna	70
070202 Hak Capaian	70
070203 Pengurusan Kata Laluan	71
070204 <i>Clear Desk</i> dan <i>Clear Screen</i>	71
0703 Kawalan Capaian Rangkaian	72
070301 Capaian Rangkaian	72
070302 Capaian Internet	73
0704 Kawalan Capaian Sistem Pengoperasian.....	74
070401 Capaian Sistem Pengoperasian	74
070402 Prasarana Kekunci Awam (PKI)	75
0705 Kawalan Capaian Aplikasi dan Maklumat	76
070501 Capaian Aplikasi dan Maklumat.....	76
0706 Peralatan Mudah Alih Dan Kerja Jarak Jauh	76
070601 Peralatan Mudah Alih.....	77
070602 Kerja Jarak Jauh.....	77
 PERKARA 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT	 79
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi.....	79
080101 Keperluan Keselamatan Sistem Maklumat	79
080102 Pengesahan Data Input dan Output.....	80
0802 Kawalan Kriptografi.....	80
080201 Enkripsi.....	80
080202 Tandatangan Digital	80
080203 Pengurusan Prasarana Kekunci Awam (PKI)	80
0803 Keselamatan Fail Sistem	81
080301 Kawalan Fail Sistem.....	81
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	81
080401 Prosedur Kawalan Perubahan	81
080402 Pembangunan Perisian Secara <i>Outsource</i>	82

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	8 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0805 Kawalan Teknikal Keterdedahan (<i>Vulnerability</i>)	82
080501 Kawalan dari Ancaman Teknikal.....	82
080502 Sekatan dalam Instalasi Perisian	83
 PERKARA 09 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT	85
0901 Mekanisme Pelaporan Insiden Keselamatan ICT	85
090101 Mekanisme Pelaporan.....	85
0902 Pengurusan Maklumat Insiden Keselamatan ICT	86
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT.....	86
090202 Penilaian Dan Keputusan Terhadap Insiden Keselamatan ICT	87
090203 Tindakbalas Terhadap Insiden Keselamatan ICT.....	87
 PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	90
1001 Dasar Kesinambungan Perkhidmatan.....	90
100101 Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana ICT (DRP).....	90
100102 Ketersediaan Fasiliti Pemprosesan Maklumat (Tambahan).....	90
 PERKARA 11 : PEMATUHAN	93
1101 Pematuhan dan Keperluan Perundangan	93
110101 Pematuhan Dasar	93
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	93
110103 Pematuhan Keperluan Audit.....	94
110104 Keperluan Perundangan.....	94
110105 Pelanggaran Perundangan	94
 PERKARA 12 : GLOSARI.....	96
LAMPIRAN 1	99
LAMPIRAN 2: PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT AADK100	
LAMPIRAN 3: SENARAI PERUNDANGAN DAN PERATURAN	102

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	9 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

A. PENGENALAN

Kerajaan sedar akan kepentingan dan tanggungjawab bagi memastikan keselamatan aset teknologi maklumat dan komunikasi (*Information and Communications Technology*), ringkasnya ICT, yang merangkumi data atau maklumat, perkakasan, perisian, sistem sokongan dan manusia (yang mengendalikan aset ICT) perlu dikawal dan dipelihara. Tanggungjawab ini harus dipikul oleh penjawat awam atau sesiapa sahaja yang menggunakan aset ICT Kerajaan selaras dengan motto Agensi iaitu '**Keselamatan Tanggungjawab Bersama**'.

'**Dasar Keselamatan ICT (DKICT) Agensi Antidadah Kebangsaan (AADK)**' mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi semasa menggunakan aset ICT AADK. Dasar ini juga menerangkan tanggungjawab dan peranan semua pengguna dalam melindungi aset ICT Kerajaan.

B. OBJEKTIF

Dasar Keselamatan ICT AADK diwujudkan untuk menjamin kesinambungan urusan AADK dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi AADK. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Manakala, objektif utama Keselamatan ICT AADK ialah seperti berikut:

- (a) Memastikan kelancaran operasi AADK dan meminimumkan kerosakan atau kemusnahan;
- (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
- (c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	10 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

C. PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

- (a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- (b) Menjamin setiap maklumat adalah tepat dan sempurna;
- (c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
- (d) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

- (a) **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- (b) **Integriti** - Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
- (c) **Tidak Boleh Disangkal** - Punca data dan maklumat hendaklah 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 menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	11 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

D. SKOP

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

- (a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
- (b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

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

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan AADK. Contohnya komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

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

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	12 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

(d) Data atau Maklumat

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

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

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

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	13 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

E. PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT AADK dan perlu dipatuhi adalah seperti berikut:

(a) Akses atas dasar perlu mengetahui

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

(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 mewujudkan, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) Akauntabiliti

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

- (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- (ii) Memeriksa maklumat dan menentukan ianya tepat dan lengkap;
- (iii) Menentukan maklumat sedia untuk digunakan;
- (iv) Menjaga kerahsiaan kata laluan;
- (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- (vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- (vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	14 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

(d) Pengasingan

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

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) Pematuhan

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

(g) Pemulihan

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

(h) Saling Bergantungan

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	15 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

F. PENILAIAN RISIKO KESELAMATAN ICT

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

AADK hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko. Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat AADK termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

AADK bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. AADK perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

- (a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
- (b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
- (c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
- (d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

G. MAKLUMAT LANJUT

Sebarang pertanyaan mengenai kandungan dokumen ini atau permohonan untuk keterangan lanjut, boleh disalurkan kepada Unit Keselamatan ICT, BTMK AADK di e-mel ukict@adk.gov.my. Dasar Keselamatan ICT AADK ini juga boleh diakses di Laman Web Rasmi AADK di www.adk.gov.my

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	16 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

H. DASAR WAJIB DAN TERPAKAI

Dasar ini adalah wajib dan terpakai kepada setiap pegawai dan kakitangan AADK, pembekal, pakar runding dan pihak-pihak lain yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT AADK, yakni **KERAJAAN MALAYSIA**. Pengguna bertanggungjawab untuk membaca, memahami dan menandatangani '**Surat Akuan Pematuhan Dasar Keselamatan ICT**' Agensi Antidadah Kebangsaan (AADK).

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	17 dari 103



DASAR KESELAMATAN ICT

AGENSI ANTIDADAH KEBANGSAAN

PERKARA 01:

PELAKSANAAN DAN PENYELESAIAN
DASAR KESELAMATAN

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 01 : PELAKSANAAN DAN PENYELENGGARAAN DASAR KESELAMATAN

Objektif :

DKICT AADK ini diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.

0101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah AADK selaku Pengerusi Mesyuarat Pengurusan Tertinggi (MPT). MPT ini terdiri daripada Ketua Pegawai Maklumat (CIO), Timbalan Ketua Pengarah Operasi (TKP(O)) dan semua Pengarah Bahagian.

Ketua
Pengarah
AADK

0102 Pemakaian Dasar

Dasar ini adalah terpakai kepada setiap kakitangan AADK dan pihak ketiga seperti kakitangan jabatan kerajaan lain, kakitangan swasta, orang awam, pembekal, kontraktor dan pakar runding yang berurusan dengan AADK dan tiada pengecualian diberikan.

Dasar ini perlu disebar kepada semua pengguna AADK (termasuk kakitangan, pembekal, pakar runding dan lain-lain).

Pengguna dan
Pihak Ketiga

0103 Penyebaran Dasar

Dasar ini perlu disebar kepada semua pengguna AADK (termasuk kakitangan, pembekal, pakar runding dan lain-lain).

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	19 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0104 Penyelenggaraan Dasar

Dasar Keselamatan ICT 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 berhubung dengan penyelenggaraan Dasar Keselamatan ICT AADK:

- (a) Kenal pasti dan tentukan perubahan yang diperlukan;
- (b) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	20 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 02:

PENGURUSAN KESELAMATAN ICT

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 02 : PENGURUSAN KESELAMATAN ICT

0201 Infrastruktur Organisasi Dalam

Objektif:

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

020101 Ketua Pengarah Agensi Antidadah Kebangsaan

Peranan dan tanggungjawab Ketua Pengarah AADK adalah seperti berikut:

- (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT AADK;
- (b) Memastikan semua pengguna mematuhi DKICT AADK
- (c) Memastikan semua keperluan jabatan seperti sumber kewangan, sumber manusia dan perlindungan keselamatan adalah mencukupi;
- (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT AADK; dan
- (e) Mempengerusikan Mesyuarat Pengurusan Tertinggi (MPT).

Ketua Pengarah
AADK

020102 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 dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
- (b) Menentukan keperluan keselamatan ICT;
- (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT AADK serta pengurusan risiko dan pengauditan; dan
- (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT AADK.

CIO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	22 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi AADK ialah Pengarah Teknologi Maklumat.

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

- (a) Menyelia pelaksanaan program-program keselamatan ICT AADK;
- (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT AADK;
- (c) Memastikan pelaksanaan pengurusan risiko keselamatan ICT AADK;
- (d) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
- (e) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumpkannya kepada CIO;
- (f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

ICTSO

020104 Pengurus ICT

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

- (a) Memastikan pelaksanaan DKICT AADK secara berkesan dengan mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT AADK;
- (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan AADK;
- (c) Memastikan semua kakitangan, kontraktor dan pembekal yang terlibat dengan bahagian mematuhi dasar, piawaian dan garis panduan keselamatan ICT;
- (d) Melaksanakan penilaian tahap keselamatan ICT AADK dan mencadangkan tindakan pemulihan atau pengukuhan bagi meningkatkan keselamatan infrastruktur ICT;
- (e) Melaksanakan dan mengemaskini penilaian risiko dan pelan penguraian risiko AADK; dan
- (f) Menyimpan rekod atau laporan terkini tentang insiden keselamatan ICT.

Pengurus ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	23 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

020105 Pentadbir Sistem ICT

Pentadbir Sistem ICT terdiri daripada seperti berikut:

- (a) Pentadbir Rangkaian ICT;
- (b) Pentadbir Sistem Aplikasi;
- (c) Pentadbir Laman Web;
- (d) Pentadbir Pusat Data;

Pentadbir Sistem
ICT

020106 Pentadbir Rangkaian ICT

Peranan dan tanggungjawab Pentadbir Rangkaian ICT 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;
- (f) Memastikan tiada sambungan rangkaian yang tidak sah; dan
- (g) Menyediakan zon rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian jika berkaitan.

Unit Pusat Data,
Rangkaian dan
Pemulihan
Bencana ICT

020107 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;

Pentadbir Sistem
Aplikasi

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	24 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|--|--|
| (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 <i>virus pattern</i> , <i>hotfix</i> dan <i>patch</i> yang berkaitan dengan sistem aplikasi terkemaskini supaya terhindar daripada ancaman virus dan penggodam; | |
| (i) | Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam mewujudkan akaun pengguna ke atas setiap sistem aplikasi; | |
| (j) | Memastikan sandaran (<i>backup</i>) sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual; | |
| (k) | Menghadkan capaian dokumentasi sistem aplikasi bagi mengelakkan dari penyalahgunaannya; dan | |
| (l) | Melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya; | |

020108 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; | Unit Aplikasi
Dalam dan
Laman Web |
| (b) | Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; | |
| (c) | Mengambil tindakan pengukuhan berdasarkan laporan insiden keselamatan yang diterima berkenaan capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; | |
| (d) | Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; | |
| (e) | Melaksanakan <i>housekeeping</i> keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di <i>web server</i> ; dan | |
| (f) | Melaksanakan proses <i>backup</i> dan <i>restoration</i> secara berkala; | |

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	25 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

020109 Pentadbir Pusat Data

Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut:

- (a) Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;
- (b) Memastikan keselamatan aset ICT yang berada dalam Pusat Data;
- (c) Melaksanakan pemulihan bencana mengikut Pelan Pemulihan Bencana (DRP) ICT AADK;
- (d) Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan.

Unit Pusat Data,
Rangkaian dan
Pemulihan
Bencana ICT

020110 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 senarai pengguna yang terlibat di dalam Latihan Pengguna;
- c) Penguatkuasaan penggunaan sistem di kalangan pengguna;
- d) Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan
- e) Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pentadbir Sistem ICT.

Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan tadbir urus sistem tersebut.

Pemilik Sistem

RUJUKAN

VERSI

TARIKH

M/SURAT

DKICT AADK

5.0

1 APRIL 2021

26 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

020111 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:

JICTA

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).

Bidang kuasa:

- a) Menetapkan hala tuju dan strategi untuk pelaksanaan ICT di AADK;
- b) Merancang, menyelaraskan 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;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	27 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- d) Meluluskan perolehan ICT bagi AADK berdasarkan keperluan sebenar dengan perbelanjaan yang berhemah serta mematuhi pekeling/peraturan semasa yang berkaitan; dan
- e) Menyelaraskan dan mengemukakan laporan perolehan ICT AADK kepada Urus Setia JPICT KDN mengikut tempoh yang telah ditetapkan.

0202 Pasukan Tindak Balas Insiden Keselamatan ICT 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);
5. Unit Aplikasi Dalaman dan Laman Web (wakil yang dilantik).

CERT AADK

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 samada sebagai input atau untuk tindakan seterusnya;
- (e) Menasihat pejabat-pejabat di bawah AADK mengambil tindakan pemulihan dan pengukuhan;
- (f) Menyebarkan makluman berkaitan dengan agensi di bawah kawalannya; dan
- (g) Menjalankan penilaian dalaman untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	28 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0203 Pihak Ketiga

Objektif:

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

020301 Keperluan Keselamatan Melibatkan Kontrak 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:

CIO, ICTSO,
Pentadbir
Sistem ICT dan
Pihak Ketiga

- a) Penjagaan kerahsiaan maklumat Kerajaan yang meliputi maklumat terperinci terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
- b) Penjagaan kerahsiaan kata laluan;
- c) Maklumat berkaitan hendaklah tepat dan lengkap dari semasa ke semasa;
- d) Penjagaan kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum;
- e) Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya;
- f) Pihak Ketiga yang menggunakan perkhidmatan ICT dan mempunyai peranan seperti berikut:
 - Tapisan keselamatan dilaksanakan sekiranya dikehendaki berurusan dengan maklumat rasmi terperinci melalui Sistem *e-Vetting* (jika berkenaan) dan Perakuan Akta Rahsia Rasmi 1972;
 - Pelaksanaan prinsip-prinsip Dasar Keselamatan ICT AADK dan menjaga kerahsiaan maklumat AADK; dan
 - Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT AADK sebagaimana **Lampiran 1**.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	29 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Perkara yang perlu dipatuhi oleh Pentadbir Sistem ICT AADK berhubung keperluan keselamatan kontrak dengan pihak ketiga termasuk yang berikut:

- (a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran akses kepada pihak ketiga;
- (b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran akses atau penggunaan kepada pihak ketiga;
- (c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut perlu dimasukkan di dalam perjanjian yang dimeterai:
 - Dasar Keselamatan ICT AADK;
 - Tapisan Keselamatan melalui sistem *e-Vetting*; dan
 - Perakuan Akta Rahsia Rasmi 1972.

020302 Keselamatan Maklumat Dalam Pengurusan Projek

Seksyen ini bertujuan untuk memastikan setiap pengurusan projek (tanpa mengira jenis projek) yang dilaksanakan oleh AADK mengambil kira aspek keselamatan maklumat secara holistik.

CIO / ICTSO adalah bertanggungjawab untuk:

- (a) Menjadikan objektif keselamatan maklumat sebahagian daripada objektif projek;
- (b) Melaksanakan penilaian terhadap risiko keselamatan maklumat di fasa awal pelaksanaan projek sebelum kawalan keselamatan yang berkaitan dikenalpasti;
- (c) Menjadikan isu keselamatan maklumat sebagai agenda dalam setiap fasa kaedah pelaksanaan projek;
- (d) Memastikan pengurusan projek mematuhi manual keselamatan dan polisi DKICT dalam setiap aktiviti pengurusan projek;
- (e) Memastikan pengurus projek telah mendapat latihan kesedaran dan pendedahan yang mencukupi berkenaan tanggungjawab untuk memastikan keselamatan maklumat sentiasa terjamin;

CIO / ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	30 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|---|--|
| (f) | Memastikan aktiviti bagi menjamin keselamatan maklumat dinyatakan secara jelas dalam jadual perancangan pelaksanaan projek; | |
| (g) | Memastikan semua pihak yang terlibat dalam sesuatu projek maklum tentang arahan berkaitan keselamatan maklumat dan mereka diikat dengan perjanjian (seperti Akta Rahsia Rasmi). | |
| (h) | ICTSO bertanggungjawab menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT. | |

020303 Polisi Keselamatan Maklumat Berkaitan Hubungan Pembekal

Seksyen ini menjelaskan keperluan untuk mendokumentasikan strategi mitigasi risiko keselamatan maklumat bila mana pembekal dibenarkan untuk akses kepada aset maklumat AADK.

CIO / ICTSO

CIO / ICTSO adalah bertanggungjawab untuk:

- | | | |
|----|---|--|
| a) | Menenalpasti dan mendokumenkan jenis-jenis pembekal (seperti khidmat servis IT, pembekal infrastruktur IT, logistik, kewangan dan sebagainya); | |
| b) | Menalpasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; | |
| c) | Mengadakan latihan kesedaran kepada semua pihak yang terlibat (AADK dan pembekal) untuk mendedahkan mereka dengan polisi, proses, dan prosedur berkaitan keselamatan maklumat. | |
| d) | Mewujudkan mekanisma/proses pengurusan pembekal dengan mengambil kira aspek keselamatan maklumat sebagai teras; | |
| e) | Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan maklumat. Proses dan prosedur berkaitan perlu diwujudkan; | |

RUJUKAN

VERSI

TARIKH

M/SURAT

DKICT AADK

5.0

1 APRIL 2021

31 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|----|--|--|
| f) | Mewujudkan kontrak rasmi bersama pembekal yang dapat menjamin keselamatan maklumat AADK di samping segala urusan bersama pembekal hendaklah dilaksanakan secara rasmi; | |
| g) | Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan maklumat yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semua aset maklumat sekiranya kontrak mereka tamat atau ditamatkan. | |

020304 Rangkaian Pembekal ICT

Seksyen ini menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan maklumat berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira.

CIO / ICTSO

CIO / ICTSO adalah bertanggungjawab untuk :

- | | | |
|-----|---|--|
| (a) | Mengenalpasti keperluan keselamatan maklumat khusus berkaitan dengan perolehan rangkaian pembekal servis ICT dan produk sebagai tambahan kepada keperluan umum keselamatan maklumat berkaitan hubungan pembekal yang telah dikenal pasti; | |
| (b) | Memastikan rangkaian pembekal yang terlibat dalam menyediakan khidmat servis ICT berkongsi hal berkaitan keselamatan maklumat (polisi, prosedur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal; | |
| (c) | Khusus untuk rangkaian pembekal produk, AADK perlu memastikan pembekal utama berkongsi praktis pembangunan produk AADK di kesemua peringkat pembekal bagi memastikan keselamatan maklumat terjamin; | |
| (d) | Melaksanakan proses pemantauan rangkaian pembekal servis ICT dan produk dengan kaedah yang berkesan bagi menjamin keperluan keselamatan maklumat sentiasa dipatuhi; | |
| (e) | Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai; | |

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	32 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|--|--|
| (f) | Mewujudkan peraturan yang khusus bagi mengawal perkongsian maklumat di kalangan rangkaian pembekal; | |
| (g) | Mewujudkan mekanisma/proses khusus untuk mengurus rangkaian pembekal khidmat servis ICT dan produk bagi memastikan keselamatan maklumat terjamin. Mekanisma yang diwujudkan wajar mampu untuk mengurus risiko sekiranya komponen produk yang dibekalkan tidak lagi boleh dibekalkan kerana perubahan trend dan teknologi yang berlaku. | |

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	33 dari 103



DASAR KESELAMATAN ICT

AGENSI ANTIDADAH KEBANGSAAN

PERKARA 03:

PENGURUSAN ASET

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 03 : PENGURUSAN ASET

Objektif :

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

0301 Akauntabiliti Aset ICT

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

030101 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 dalam Kad Daftar Harta Modal dan Inventori sebagaimana mengikut Pekeliling Perbendaharaan Bil. 5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan (TPA);
- (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;
- (d) Memastikan semua peraturan pengendalian aset ICT dikenalpasti, didokumen dan dilaksanakan; dan
- (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.

Pegawai
Aset dan
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	35 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0302 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

- (a) Rahsia Besar;
- (b) Rahsia;
- (c) Sulit; atau
- (d) Terhad.

Semua
Pengguna

0303 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, 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 ICT yang ditetapkan;
- (f) Melaksanakan peraturan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

Semua
Pengguna

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

36 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 04:

KESELAMATAN SUMBER MANUSIA

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 04 : KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia

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 warga AADK hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

0402 Sebelum Berkhidmat

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;
- (b) Menjalankan tapisan keselamatan untuk warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan selaras dengan keperluan perkhidmatan; dan
- (c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Semua
Pengguna

0403 Dalam Perkhidmatan

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;
- (b) 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;

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	38 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|---|--|
| <p>(c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga AADK, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sekiranya berlaku pelanggaran dasar dengan perundangan dan peraturan ditetapkan Agensi; dan</p> <p>(d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Cawangan Pengurusan Sumber Manusia, Bahagian Khidmat Pengurusan AADK.</p> | |
|---|--|

0404 Bertukar Atau Tamat Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

- | | |
|---|----------------|
| <p>(a) Memastikan semua aset ICT dikembalikan kepada AADK mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan</p> <p>(b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan Agensi dan/atau terma perkhidmatan.</p> | Semua Pengguna |
|---|----------------|

0405 Program Kesedaran, Pendidikan Dan Latihan Keselamatan ICT

Setiap pengguna perlu diberikan kesedaran, latihan atau kursus mengenai keselamatan ICT yang bersesuaian dengan peranan dan tanggungjawab masing-masing secara berterusan.	Semua Pengguna
--	----------------

Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT AADK dan Kerajaan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	39 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 05:

**KESELAMATAN FIZIKAL DAN
PERSEKITARAN**

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif :

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

050101 Kawalan Kawasan

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

Pegawai
Keselamatan
Jabatan, CIO,
ICTSO dan
Pentadbir
Pusat Data.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- (c) Memasang alat penggera atau kamera;
- (d) Mengehadkan jalan keluar masuk;
- (e) Mewujudkan perkhidmatan kawalan keselamatan;
- (f) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- (g) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan mengikut Arahan Keselamatan Kerajaan; dan
- (h) Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;
- (i) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	41 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

050102 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (a) Setiap pengguna AADK hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
- (b) Semua pas keselamatan hendaklah diserahkan balik kepada AADK apabila pengguna berhenti atau bersara;
- (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu masuk utama premis-premis AADK. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan
- (d) Kehilangan pas mestilah dilaporkan dengan segera.

Semua
Pengguna

050103 Kawasan Larangan

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

Kawasan larangan di AADK adalah seperti berikut:

- i. Bilik Ketua Pengarah;
- ii. Bilik Timbalan Ketua Pengarah Pengurusan,
- iii. Bilik Timbalan Ketua Pengarah Operasi;
- iv. Bilik semua Pengarah Bahagian;
- v. Pusat Data (*Data Centre*) dan
- vi. Kawasan-kawasan lain yang dikategorikan sebagai Kawasan Larangan oleh AADK.

- (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.

Pentadbir
Sistem

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	42 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0502 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT AADK dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

050201 Peralatan ICT

Perkara-perkara yang perlu dipatuhi termasuk yang berikut :

- (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 Pentadbir Sistem ICT;
- (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;

Semua
Pengguna

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

43 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (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, perlulah 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 berkuatkuasa;
- (n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;
- (o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem 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 Pentadbir Sistem ICT;
- (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;
- (u) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan
- (v) Memastikan *plug* dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	44 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

050202 Media Storan

Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain.

Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
- (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
- (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
- (e) Akses dan pergerakan media storan hendaklah direkodkan;
- (f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal;
- (g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data;
- (h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan
- (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	45 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

050203 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;
- (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan
- (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.

Semua
Pengguna

050204 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan AADK;
- (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO/ICTSO;
- (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-ROM, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan
- (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan

Semua
Pengguna

050205 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;

Pegawai Aset
serta
Unit Teknikal
dan Helpdesk

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	46 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|---|--|
| <ul style="list-style-type: none"> (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada ICTSO. | |
|---|--|

050206 Peralatan di Luar Premis

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; (b) Peralatan perlu dilindungi dan dikawal sepanjang masa; (c) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; (d) Memastikan aktiviti pinjaman dan pemulangan perkakasan ICT direkodkan; dan (e) Memastikan perkakasan ICT yang dipulangkan dalam keadaan baik dan lengkap.	Semua Pengguna
---	---------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	47 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

050207 Pelupusan Perkakasan

Pelupusan 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.

Semua
Pengguna
dan
Pegawai Aset

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan AADK.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;
- (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan ke dalam media storan yang dibenarkan;
- (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
- (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
- (e) Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan dan mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
- (f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori;
- (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	48 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|---|--|
| (h) | <p>Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:</p> <ol style="list-style-type: none"> i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, <i>hardisk</i>, <i>motherboard</i> dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di AADK; iii. Memindah keluar dari AADK mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab AADK; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau <i>thumb drive</i> sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan. | |
|-----|---|--|

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT AADK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT AADK, semua cadangan perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK).

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	49 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Merancang dan menyediakan pelan keseluruhan pusat data termasuk ruang peralatan komputer, ruang percetakan dan ruang atur pejabat;
- (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) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- (d) Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT;
- (e) Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT; dan
- (f) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran perkakasan komputer.

050302 Bekalan Kuasa

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

Pentadbir
Pusat Data

Perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Melindungi semua peralatan ICT AADK dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;
- (b) Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; dan
- (c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	50 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

050303 Kabel

Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah.

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.

050304 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Pelan Laluan Kecemasan Kebakaran AADK; dan
- (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) AADK yang dilantik mengikut aras.

Semua
Pengguna
dan
Pegawai
Keselamatan
Jabatan

050305 Utiliti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Semua kemudahan sistem seperti penghawa dingin, bekalan air, kumbahan dan pengalihan udara perlu dilindungi dari kegagalan bekalan elektrik dan sebarang gangguan; dan

Semua
Pengguna
dan Pegawai
Keselamatan
Jabatan

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	51 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|--|--|
| (b) Kemudahan sistem perlu diperiksa dan diuji agar sentiasa berfungsi dengan baik bagi mengurangkan risiko kegagalan; | |
|--|--|

0504 Keselamatan Dokumen

Objektif:

Melindungi maklumat AADK dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuai.

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- | | |
|--|----------------|
| <ul style="list-style-type: none"> (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pengekalan dan pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. | Semua Pengguna |
|--|----------------|

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

52 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 06:

PENGURUSAN OPERASI DAN KOMUNIKASI

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Pengendalian Prosedur

Objektif :

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

060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Semua prosedur pengurusan operasi yang diwujudkan, dikenalpasti dan digunakan 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

060102 Kawalan Perubahan

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;
- (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	54 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

060103 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
- (b) Mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperinci atau dimanipulasi; dan
- (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

Semua
Pengguna

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga

060201 Perkhidmatan Penyampaian

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;

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	55 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|---|--|
| (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. | |

0603 Perancangan Dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Perancangan 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 ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

Pentadbir
Sistem ICT
dan
ICTSO

060302 Penerimaan Sistem

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

Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

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

Pentadbir
Sistem ICT
dan
ICTSO

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

56 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

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

0604 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, sistem dan sebagainya.

060401 Perlindungan Perisian Berbahaya

Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

- (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;
- (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa;
- (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
- (d) Mengemaskini anti virus 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 sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
- (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;

Bahagian
Teknologi
Maklumat &
Komunikasi

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	57 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|--|--|
| (h) | Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan | |
| (i) | Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. | |

060402 Perlindungan dari *Mobile Code*

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

Semua
Pengguna

0605 Housekeeping

Objektif:

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

060501 Penduaan (*Backup*)

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah.

Pentadbir
Sistem ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- | | | |
|-----|--|--|
| (a) | Membuat <i>backup</i> keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; | |
| (b) | Membuat <i>backup</i> ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat; | |
| (c) | Menguji sistem <i>backup</i> dan <i>restore</i> sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan | |
| (d) | Merekod dan menyimpan salinan <i>backup</i> di lokasi yang selamat. | |

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

58 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0606 Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

060601 Kawalan Infrastruktur Rangkaian

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

Pentadbir
Rangkaian
ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan 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 serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian ICT;
- (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 mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat AADK;
- (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	59 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|--|--|
| <ul style="list-style-type: none"> (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; dan (l) Kemudahan bagi <i>wireless</i> LAN perlu dipastikan kawalan keselamatan. | |
|--|--|

0607 Pengurusan Media

Objektif:

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

060701 Penghantaran dan Pemindahan

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

Semua
Pengguna

060702 Prosedur Pengendalian Media

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

- | | |
|---|-------------------|
| <ul style="list-style-type: none"> (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; (e) Menyimpan semua media di tempat yang selamat; dan | Semua
Pengguna |
|---|-------------------|

RUJUKAN

DKICT AADK

VERSI

5.0

TARIKH

1 APRIL 2021

M/SURAT

60 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|--|--|
| (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat. | |
|--|--|

060703 Keselamatan Sistem Dokumentasi

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

	Semua Pengguna
--	----------------

- | | |
|---|--|
| (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
(b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan
(c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada. | |
|---|--|

0608 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara AADK dan agensi luar terjamin.

060801 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	
---	--

	Semua Pengguna
--	----------------

- | | |
|--|--|
| (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;
(b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara AADK dengan agensi luar;
(c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari AADK; dan | |
|--|--|

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	61 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

060802 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di AADK hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan 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 keipilan, 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;
- (g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	62 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|---|--|
| <ul style="list-style-type: none"> (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 <i>mailbox</i> 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. | |
|---|--|

0609 Perkhidmatan e-Dagang (*Electronic Commerce Services*)

Objektif:

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

060901 E-Dagang

Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.

Semua
Pengguna

Perkara yang mesti dipatuhi termasuk yang berikut :

- (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	63 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | |
|---|--|
| <p>(b) Maklumat yang terlibat dalam transaksi dalam talian (<i>on-line</i>) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan</p> <p>(c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.</p> | |
|---|--|

060902 Maklumat Umum

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

- | | |
|--|----------------|
| <p>(a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;</p> <p>(b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan</p> <p>(c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.</p> | Semua Pengguna |
|--|----------------|

0610 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut:	
--	--

- | | |
|--|-------|
| <p>(a) Sebarang percubaan pencerobohan kepada sistem ICT AADK;</p> | ICTSO |
|--|-------|

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	64 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);
- (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;
- (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;
- (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;
- (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian;
- (g) Aktiviti penyalahgunaan akaun e-mel; dan
- (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian ICT.

061002 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut:

- (a) Rekod setiap aktiviti transaksi;
- (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;
- (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
- (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

Pentadbir
Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	65 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.

061003 Sistem Log

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 ICTSO dan CIO.

Pentadbir
Sistem ICT

061004 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 diwujudkan dan hasilnya perlu dipantau secara berkala;
- (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan;
- (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan;
- (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan

Bahagian
Teknologi
Maklumat
Dan
Komunikasi

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	66 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|--|--|
| (f) | Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam AADK atau domain keselamatan perlu diselaraskan ke Pelayan NTP (<i>Network Time Protocol</i>). | |
|-----|--|--|

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	67 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 07:

KAWALAN CAPAIAN

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 07 : KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat.

070101 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.

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) Kawalan ke atas kemudahan pemprosesan maklumat.

Bahagian
Teknologi
Maklumat
Dan
Komunikasi,
ICTSO

0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT AADK.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	69 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

070201 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan.

Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

- (a) Akaun yang diperuntukkan oleh AADK sahaja boleh digunakan;
- (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;
- (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik 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) 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, boleh membekukan akaun pengguna yang bercuti atau berkursus panjang.

Semua
Pengguna
dan
Pentadbir
Sistem ICT

070202 Hak Capaian

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

Pentadbir
Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	70 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

070203 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh AADK seperti berikut:

Semua
Pengguna
dan
Pentadbir
Sistem ICT

- (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;
- (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;
- (i) Tentukan had masa pengesahan maksima adalah sepuluh (10) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; dan
- (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian;

070204 Clear Desk dan Clear Screen

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

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	71 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

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 bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
- (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faks dan mesin fotostat.

0703 Kawalan Capaian Rangkaian

Objektif:

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

070301 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- (a) Menempatkan atau memasang antara muka 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
- (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

Pentadbir
Sistem ICT
dan
ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	72 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

070302 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Penggunaan Internet di AADK hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian AADK;
- (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;
- (c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;
- (d) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah / pegawai yang diberi kuasa;
- (e) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;
- (f) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet;
- (g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
- (h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh AADK;
- (i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;
- (j) Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

Pentadbir
Rangkaian

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	73 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut:
- i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan
 - ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

0704 Kawalan Capaian Sistem Pengoperasian

Objektif:

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

070401 Capaian Sistem Pengoperasian

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

Kemudahan ini juga perlu bagi:

- (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan
- (b) Merekodkan capaian yang berjaya dan gagal.

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

- (a) Mengesahkan pengguna yang dibenarkan;
- (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan
- (c) Menjana amaran (*alert*) sekiranya berlaku pelanggaran ke atas peraturan keselamatan sistem.

Pentadbir
Sistem ICT
dan
ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	74 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;
- (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
- (c) Mengehadkan dan mengawal penggunaan program; dan
- (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

070402 Prasarana Kekunci Awam (PKI)

Public Key Infrastructure (PKI) atau Prasarana Kekunci Awam adalah gabungan perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan komunikasi dan transaksi urus niaga dalam internet. Bagi melakukan transaksi selamat, prasarana Kekunci Awam seperti PKI token merupakan satu kemudahan bagi menjamin integriti data yang dihasilkan melalui sistem aplikasi menggunakan kaedah pengesahan pengenalan identiti pengguna dan tandatangan digital.

Semua
Pengguna

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;
- (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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	75 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0705 Kawalan Capaian Aplikasi dan Maklumat

Objektif:

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

070501 Capaian Aplikasi dan Maklumat

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

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

- (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan;
- (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log sistem);
- (c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
- (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
- (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah terhad kepada perkhidmatan yang dibenarkan sahaja.

Pentadbir
Sistem ICT
dan
ICTSO

0706 Peralatan Mudah Alih Dan Kerja Jarak Jauh

Objektif:

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	76 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

070601 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan;
- (b) Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan;

Semua
Pengguna

070602 Kerja Jarak Jauh

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	77 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 08:

**PEROLEHAN, PEMBANGUNAN DAN
PENYELENGGARAAN SISTEM
MAKLUMAT**

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 08 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

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

080101 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira 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,
Pentadbir
Sistem ICT
dan
ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	79 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

080102 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan
- (b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

Pemilik
Sistem dan
Pentadbir
Sistem ICT

0802 Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

080201 Enkripsi

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

Semua
Pengguna

080202 Tandatangan Digital

Penggunaan tandatangan digital adalah digalakkan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.

Semua
Pengguna

080203 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.

Semua
Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	80 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

0803 Keselamatan Fail Sistem

Objektif:

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

080301 Kawalan Fail Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Proses pengemaskinian fail sistem 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;
- (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian;
- (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan
- (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

Pemilik Sistem
dan Pentadbir Sistem ICT

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 Prosedur Kawalan Perubahan

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;

Pemilik Sistem
dan Pentadbir Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	81 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (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;
- (d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan
- (e) Menghalang sebarang peluang untuk membocorkan maklumat.

080402 Pembangunan Perisian Secara *Outsource*

Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem dan Pentadbir Sistem ICT.

Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik AADK.

Pemilik
Sistem,
Pentadbir
Sistem ICT
dan pihak
Ketiga

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:

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

080501 Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.

Pentadbir
Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	82 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Perkara yang perlu dipatuhi adalah seperti berikut:

- (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;
- (b) Menilai tahap pendedahan bagi mengenalpasti tahap risiko yang bakal dihadapi; dan
- (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

080502 Sekatan dalam Instalasi Perisian

Seksyen ini menjelaskan peraturan berhubung instalasi perisian yang perlu diwujudkan dan dilaksanakan.

Unit Teknikal
dan Helpdesk

Perkara-perkara yang perlu dipatuhi tetapi tidak hanya terhad kepada yang berikut:

- (a) Polisi yang jelas berkaitan jenis perisian yang dibenar (seperti patch keselamatan untuk perisian sedia ada) dan tidak dibenarkan (seperti perisian untuk kegunaan peribadi) untuk instalasi perlu dipatuhi; dan
- (b) Prinsip keutamaan rendah wajar diadaptasi dalam peraturan instalasi perisian. Jika sesuatu keizinan diberikan, kemampuan pengguna perlu dipastikan untuk melaksanakan proses instalasi.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	83 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 09:

**PENGURUSAN PENGENDALIAN INSIDEN
KESELAMATAN ICT**

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 09 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif :

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

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT ataupun ancaman berkemungkinan berlakunya suatu kejadian. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat.

Semua
Pengguna

Insiden keselamatan ICT 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 mencerooboh, penyelewengan dan insiden yang tidak dijangka.

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di AADK sepertimana **Lampiran 2**.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	85 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

- (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
- (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

0902 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

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

090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran. Maklumat ini juga adalah bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Selain itu, ia juga bagi mengenalpasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada AADK. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan diselenggarakan.

Kawalan-kawalan yang perlu diambil kira 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) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- (c) Menyediakan pelan kontingensi dan mengaktifkan Pelan Kesenambungan Perkhidmatan;
- (d) Menyediakan tindakan pemulihan segera; dan

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	86 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

090202 Penilaian Dan Keputusan Terhadap Insiden Keselamatan ICT

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;
- (c) Hasil daripada penilaian yang dibuat boleh dipanjangkan kepada CERT supaya pengesahan atau penilaian semula dapat dilakukan;
- (d) Hasil daripada penilaian juga perlu direkodkan dengan terperinci untuk rujukan masa depan dan penentusahan.

090203 Tindakbalas Terhadap Insiden Keselamatan ICT

Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya oleh pihak yang bertanggungjawab mengikut prosedur yang berkaitan. Matlamat utama tindakbalas terhadap insiden keselamatan ICT adalah untuk mengembalikan tahap keselamatan ke paras normal dan seterusnya melaksanakan langkah-langkah perlu pemulihan.

Pasukan tindakbalas wajar melaksanakan perkara berikut:

- (a) Mengumpul bahan bukti secepat yang mungkin selepas kejadian;
- (b) Melaksanakan forensik keselamatan maklumat;
- (c) Insiden dimaklumkan kepada pihak yang berkaitan atau perlu tahu;
- (d) Semua aktiviti dalam memberi tindakbalas direkod secara sistematik untuk analisis selanjutnya;
- (e) Mengendalikan dengan efektif kelemahan-kelemahan keselamatan maklumat yang diketahui menjadi penyebab atau penyumbang kepada sesuatu insiden berlaku;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	87 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

- | | | |
|-----|---|--|
| (f) | Selepas sesuatu insiden ditangani dengan sempurna, penutupan kes secara rasmi perlu dilakukan dengan rekod; | |
| (g) | Analisa pasca insiden wajar dilakukan untuk mengenalpasti punca insiden; | |

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	88 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 10:

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif :

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

100101 Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana ICT (DRP)

PKP adalah di bawah tanggungjawab Bahagian Khidmat Pengurusan (BKP) dan DRP adalah di bawah tanggungjawab 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.

Pentadbir
Sistem ICT

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; dan
- (d) Mengadakan program latihan/simulasi kepada pengguna mengenai prosedur pemulihan bencana sekurang-kurangnya setahun sekali.

100102 Ketersediaan Fasiliti Pemprosesan Maklumat (Tambahan)

Untuk memastikan kebolehsediaan fasiliti pemprosesan maklumat di tahap yang tinggi, kaedah pemprosesan bertindan (lebih dari satu lokasi/platform pemprosesan) perlu diwujudkan.

ICTSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	90 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

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;
- (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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	91 dari 103



DASAR KESELAMATAN ICT

AGENSI ANTIDADAH KEBANGSAAN

PERKARA 11:

PEMATUHAN

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 11 : PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif :

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT AADK.

110101 Pematuhan Dasar

Setiap pengguna di AADK hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT AADK dan undang-undang atau peraturan-peraturan lain yang berkaitan yang telah dikuat kuasakan.

Semua
Pengguna

Semua aset ICT di AADK termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT AADK yang digunakan berlainan dengan maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber AADK.

110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

ICTSO

Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	93 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua Pengguna
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di AADK adalah seperti di Lampiran 3 .	Semua Pengguna
110105 Pelanggaran Perundangan	
Pelanggaran Dasar Keselamatan ICT AADK boleh dikenakan tindakan tatatertib.	Semua Pengguna

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	94 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 12:

GLOSARI

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

PERKARA 12 : GLOSARI

(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) **Ancaman**

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

(d) **Vulnerability**

Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.

(e) **Insiden Keselamatan**

Bermaksud musibah (*adverse event*) yang berlaku ke atas sistem 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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	96 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

(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 mengendalikan insiden keselamatan *ICT*.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	97 dari 103



DASAR KESELAMATAN ICT

AGENCI ANTIDADAH KEBANGSAAN

PERKARA 13:

LAMPIRAN

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

LAMPIRAN 1

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT AADK

Nama :

No. Kad Pengenalan :

Jawatan :

Jabatan / Bahagian / Unit :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT AADK; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

(Tandatangan Pegawai / Kakitangan)

Tarikh :

Disahkan Oleh :

Pegawai Keselamatan ICT (ICTSO) AADK

.....

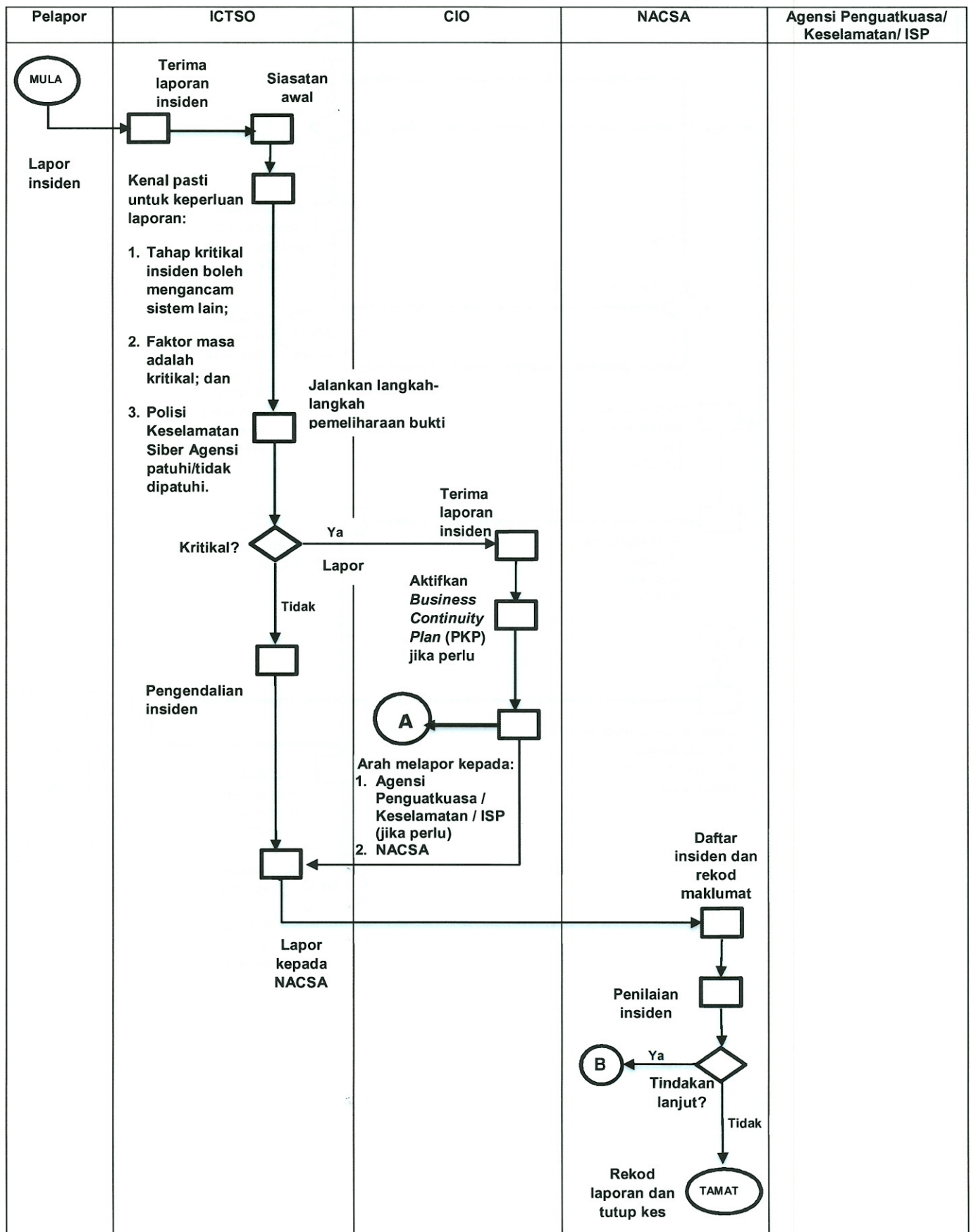
()

Tarikh :

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	99 dari 103

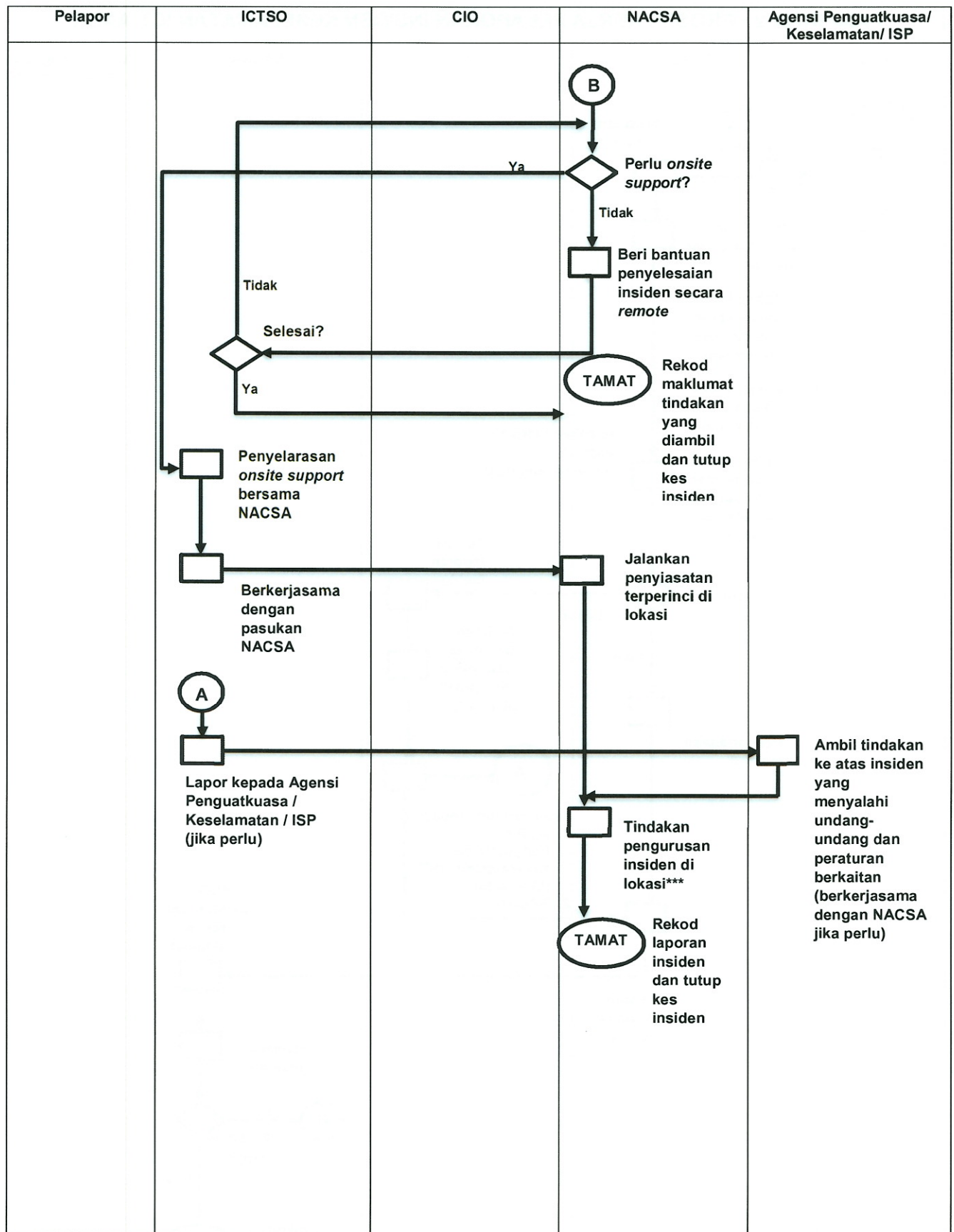
DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

LAMPIRAN 2 : PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT AADK



RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	100 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN



RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	101 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

LAMPIRAN 3 : SENARAI PERUNDANGAN DAN PERATURAN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
1.	Akta 88 - Akta Rahsia Rasmi 1972	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, Jabatan Perdana Menteri
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 AgensiAgensi 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 Kerajaan.	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
10.	Arahan Teknologi Maklumat 2007 bertarikh 19 Disember 2007.	MAMPU
11.	Arahan Amalan 2013 (Jadual Pelupusan Rekod Fungsian)	Arkib Negara Malaysia

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	102 dari 103

DASAR KESELAMATAN ICT AGENSI ANTIDADAH KEBANGSAAN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
12.	Pekeliling Perkhidmatan Bil. 5 Tahun 2007: Panduan Pengurusan Pejabat bertarikh 30 April 2007	JPA
13.	Surat Pekeliling Am Bil. 1 Tahun 1997: Peraturan Pemeliharaan Rekod-rekod Kerajaan bertarikh 11 April 1997.	Arkib Negara Malaysia
15.	Pekeliling Am Bil 3 Tahun 2009: Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 17 November 2009.	MAMPU
16.	Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000.	MAMPU
17.	Akta Hak Cipta (Pindaan) 2012 bertarikh 1 Mac 2012.	KPDNKK (Perbadanan Harta Intelek Malaysia)

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT AADK	5.0	1 APRIL 2021	103 dari 103