DASAR KESELAMATAN ICT

JABATAN WAKAF, ZAKAT DAN HAJI (JAWHAR) JABATAN PERDANA MENTERI

2 November 2017

Versi 3.0

SEJARAH DOKUMEN

Tarikh	Semakan	Kelulusan	Tarikh Kuatkuasa
Februari 2008	Versi 1.0	JPICT	Februari 2008
4 April 2014	Versi 2.0	JPICT bil 1/2014	1 Oktober 2014
2 November 2017	Versi 3.0	JPICT bil 1/2017	2 November 2017

SENARAI RINGKASAN

CIO	- *Chief Information Officer*
GCERT	- *Government Computer Emergency Response Team*
ICT	- *Information and Communication Technology*
ICTSO	- *Information Communication and Technology Security Officer*
ISMS	- *Information Security Management System*
ISP	- *Internet Service Provider*
JAWHAR	- Jabatan Wakaf, Zakat dan Haji
JPICT	- Jawatankuasa Pemandu ICT
KPKK	- Ketua Pegawai Keselamatan Kerajaan
STM	- Seksyen Teknologi Maklumat
PKI	- *Public-Key Infrastucture*

KANDUNGAN

PENGENALAN 1

OBJEKTIF 1

SKOP 1

PRINSIP - PRINSIP 1

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR 4

Dasar Keselamatan ICT 4

010101 Pelaksanaan Dasar 4

010102 Penyebaran Dasar 4

010103 Penyelenggaraan Dasar 4

010104 Pengecualian Dasar 5

PERKARA 02 ORGANISASI KESELAMATAN 5

Infrastruktur Organisasi Keselamatan 5

020101 Ketua Pengarah 5

020102 Ketua Pegawai Maklumat (CIO) 6

020103 Pegawai Keselamatan ICT (ICTSO) 7

020104 Pengurus ICT 8

020105 Pentadbir Sistem ICT 9

020106 Pentadbir Rangkaian 10

020107 Pengguna 11

Pihak Ketiga 12

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 12

PERKARA 03 KAWALAN DAN PENGELASAN ASET 14

Akauntabiliti Aset 14

030101 Inventori Aset 14

Pengelasan dan Pengendalian Maklumat 14

030201 Pengelasan Maklumat 14

030202 Pengendalian Maklumat 15

PERKARA 04 KESELAMATAN SUMBER MANUSIA 17

Keselamatan ICT Dalam Tugas Harian 17

040101 Tanggungjawab Keselamatan 17

040102 Terma dan Syarat Perkhidmatan 17

040103 Perakuan Akta Rahsia Rasmi 17

Menangani Insiden Keselamatan ICT 18

040201 Pelaporan Insiden 18

Pendidikan 19

040301 Program Kesedaran Keselamatan ICT 19

Tindakan Tatatertib 20

040401 Pelanggaran Dasar 20

PERKARA 05 KESELAMATAN FIZIKAL 21

Keselamatan Kawasan 21

050101 Perimeter Keselamatan Fizikal 21

050102 Kawalan Masuk Fizikal 22

050103 Kawasan Larangan 22

Keselamatan Peralatan 23

050201 Perkakasan 23

050202 Dokumen 24

050203 Media Storan 25

050204 Kabel 26

050205 Penyelenggaraan 26

050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat 27

050207 Peralatan di Luar Premis 27

050208 Pelupusan 28

050209 *Clear Desk* dan *Clear Screen* 28

Keselamatan Persekitaran 29

050301 Kawalan Persekitaran 29

050302 Bekalan Kuasa 30

050303 Prosedur Kecemasan 31

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI 32

Pengurusan Prosedur Operasi 32

060101 Pengendalian Prosedur 32

060102 Kawalan Perubahan 32

060103 Prosedur Pengurusan Insiden 33

Perancangan dan Penerimaan Sistem 34

060201 Perancangan Kapasiti 34

060202 Penerimaan Sistem 34

Perisian Berbahaya 35

060301 Perlindungan dari Perisian Berbahaya 35

Housekeeping 36

060401 Penduaan 36

060402 Sistem Log 37

Pengurusan Rangkaian 37

060501 Kawalan Infrastruktur Rangkaian 37

Pengurusan Laman Web 39

060601 Laman Web 39

Pengurusan Media 40

060701 Penghantaran dan Pemindahan 40

060702 Prosedur Pengendalian Media 40

060703 Keselamatan Sistem Dokumentasi 41

Keselamatan Komunikasi 42

060801 Internet 42

060802 Mel Elektronik 43

PERKARA 07 KAWALAN CAPAIAN 45

Dasar Kawalan Capaian 45

070101 Keperluan Dasar 45

Pengurusan Capaian Pengguna 45

070201 Akaun Pengguna 45

070202 Jejak Audit 46

Kawalan Capaian Sistem dan Aplikasi 47

070301 Sistem Maklumat dan Aplikasi 47

Peralatan Komputer Mudah Alih 49

070401 Penggunaan Peralatan Komputer Mudah Alih 49

PERKARA 08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 50

Keselamatan Dalam Membangunkan Sistem dan Aplikasi 50

080101 Keperluan Keselamatan 50

Kriptografi 51

080201 Penyulitan 51

080202 Tandatangan Digital 51

080203 Pengurusan Infrastruktur Kunci Awam (*PKI*) 51
Fail Sistem 52
080301 Kawalan Fail Sistem 52
Pembangunan dan Proses Sokongan 52
080401 Kawalan Perubahan 52
PERKARA 09 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 54
Dasar Kesinambungan Perkhidmatan 54
090101 Pelan Kesinambungan Perkhidmatan 54
PERKARA 10 PEMATUHAN 56
Pematuhan dan Keperluan Perundangan 56
100101 Pematuhan Dasar 56
100102 Keperluan Perundangan 56

PENGENALAN

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

OBJEKTIF

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

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan sistem) dan fizikal (contoh: komputer, peralatan komunikasi dan media storan). Dasar ini adalah terpakai oleh semua pengguna di JAWHAR termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT JAWHAR.

PRINSIP- PRINSIP

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

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan

kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kebenaran permohonan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT JAWHAR;

d. Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. 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 JAWHAR 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 jika perlu mewujudkan Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan; dan

h. Saling Bergantungan

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

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

PERKARA		TANGGUNGJAWAB
Dasar Keselamatan ICT		
010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah JAWHAR dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.	Ketua Pengarah
010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna JAWHAR (termasuk kakitangan, pembekal, pakar runding dan lain-lain.)	ICTSO
010103 Penyelenggaraan Dasar		
	Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT JAWHAR: a. Kenal pasti dan tentukan perubahan yang	ICTSO

PERKARA		TANGGUNGJAWAB
	diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c. Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104 Pengecualian Dasar		
	Dasar Keselamatan ICT JAWHAR adalah terpakai kepada semua pengguna ICT JAWHAR dan tiada pengecualian diberikan.	Semua

PERKARA 02 ORGANISASI KESELAMATAN

PERKARA		TANGGUNGJAWAB
Infrastruktur Organisasi Keselamatan		
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi		
020101 Ketua Pengarah		
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT JAWHAR; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT JAWHAR; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT JAWHAR.	Ketua Pengarah
020102 Ketua Pegawai Maklumat (CIO)		
	Timbalan Ketua Pengarah JAWHAR adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut:	CIO

PERKARA		TANGGUNGJAWAB
	a. Membantu Ketua Pengarah dalam melaksanakan tugas - tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; dan c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	
020103 Pegawai Keselamatan ICT (ICTSO)		
	Ketua Bahagian Pengarah Teknologi Maklumat adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program - program keselamatan ICT JAWHAR; b. Menguatkuasakan Dasar Keselamatan ICT JAWHAR; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JAWHAR kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JAWHAR; e. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah - langkah	ICTSO

PERKARA		TANGGUNGJAWAB
	perlindungan yang bersesuaian; f. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; g. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah - langkah baik pulih dengan segera; h. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JAWHAR; dan i. Menyedia dan melaksanakan program - program kesedaran mengenai keselamatan ICT.	
020104 Pengurus ICT		
	Ketua Seksyen Teknologi Maklumat adalah merupakan Pengurus ICT JAWHAR. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JAWHAR; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JAWHAR; c. Menentukan kawalan akses semua pengguna terhadap aset ICT JAWHAR;	Pengurus ICT

	PERKARA	TANGGUNGJAWAB
	d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JAWHAR.	
020105 Pentadbir Sistem ICT		
	Penolong Pengarah Teknologi Maklumat adalah merupakan Pentadbir Sistem ICT JAWHAR. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JAWHAR; c. Memantau aktiviti capaian harian pengguna; d. Mengenal pasti aktiviti - aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;	Pentadbir Sistem ICT, STM

	PERKARA	TANGGUNGJAWAB
	e. Menyimpan dan menganalisis rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
020106 Pentadbir Rangkaian		
	Penolong Pegawai Teknologi Maklumat (Operasi/Sokongan Teknikal) adalah merupakan Pentadbir Rangkaian. Peranan dan tanggungjawab pentadbir rangkaian adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT JAWHAR; c. Memantau aktiviti capaian rangkaian harian pengguna; d. Mengenal pasti aktiviti - aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;	Pentadbir Rangkaian, STM

	PERKARA	TANGGUNGJAWAB
	e. Menyimpan dan menganalisis rekod jejak audit; dan f. Menyediakan laporan akses rangkaian secara berkala.	
020107 Pengguna		
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT JAWHAR; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Lulus tapisan keselamatan; d. Melaksanakan prinsip - prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat JAWHAR; e. Melaksanakan langkah - langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat	Pengguna

	PERKARA	TANGGUNGJAWAB
	terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Penjaga kerahsiaan langkah - langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. Menghadiri program - program kesedaran mengenai keselamatan ICT; dan h. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT JAWHAR.	

	PERKARA	TANGGUNGJAWAB
Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak Ketiga (Pembekal, Pakar Runding dan Lain-lain)		
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga		
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut:	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pihak Ketiga

PERKARA		TANGGUNGJAWAB
	a. Membaca, memahami dan mematuhi Dasar keselamatan ICT JAWHAR; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Akses kepada aset ICT JAWHAR perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkaraperkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Dasar Keselamatan ICT JAWHAR; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek.	

PERKARA 03 KAWALAN DAN PENGELASAN ASET

PERKARA		TANGGUNGJAWAB
Akauntabiliti Aset		
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JAWHAR		
030101 Inventori Aset		
	Semua aset ICT JAWHAR hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem ICT, Pentadbir Rangkaian, Semua
Pengelasan dan Pengendalian Maklumat		
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian		
030201 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat	Semua

PERKARA		TANGGUNGJAWAB
	keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	
030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah - langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran	Semua

PERKARA		TANGGUNGJAWAB
	dan pemusnahan; dan g. Menjaga kerahsiaan langkah - langkah keselamatan ICT dari diketahui umum.	

PERKARA 04 KESELAMATAN SUMBER MANUSIA

PERKARA		TANGGUNGJAWAB
Keselamatan ICT Dalam Tugas Harian		
Objektif : Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JAWHAR		
040101 Tanggungjawab Keselamatan		
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Semua
040102 Terma dan Syarat Perkhidmatan		
	Semua warga JAWHAR yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
040103 Perakuan Akta Rahsia Rasmi		
	Warga JAWHAR yang menguruskan maklumat terperingkat hendaklah mematuhi	Semua

PERKARA		TANGGUNGJAWAB
	semua peruntukan Akta Rahsia Rasmi 1972.	
Menangani Insiden Keselamatan ICT		
Objektif: Meminimumkan kesan insiden keselamatan ICT		
040201 Pelaporan Insiden		
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak - pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak - pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden - insiden yang tidak diingini. Nota 2: Prosedur Pelaporan insiden Keselamatan ICT	Semua

PERKARA		TANGGUNGJAWAB
	berdasarkan : a. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT”. b. Surat Pekeliling Am Bilangan 4 Tahun 2006 “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam”.	
Pendidikan		
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT		
040301 Program Kesedaran Keselamatan ICT		
	Setiap pengguna di JAWHAR perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT JAWHAR.	ICTSO

PERKARA		TANGGUNGJAWAB
Tindakan Tatatertib		
Objektif: Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT JAWHAR		
040401 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT JAWHAR akan dikenakan tindakan tatatertib.	Semua

PERKARA 05 KESELAMATAN FIZIKAL

PERKARA		TANGGUNGJAWAB
Keselamatan Kawasan		
Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat		
050101 Perimeter Keselamatan Fizikal		
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah - langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a. Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera atau kamera; e. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO

PERKARA		TANGGUNGJAWAB
050102 Kawalan Masuk Fizikal		
	a. Setiap pengguna JAWHAR hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di lobi utama Blok D, Komplek Pentadbiran Islam (KIP) terlebih dahulu; e. Kehilangan pas mestilah dilaporkan dengan segera; f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JAWHAR;	Semua dan pelawat
050103 Kawasan Larangan		
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di JAWHAR adalah bilik Ketua Pengarah, Timbalan Ketua Pengarah,	Semua

PERKARA		TANGGUNGJAWAB
	Pengarah Bahagian, Ketua Seksyen, Pusat Data dan bilik kerja ICT. Akses kepada bilikbilik tersebut hanyalah kepada pegawaipegawai yang diberi kuasa sahaja : a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes - kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	
Keselamatan Peralatan		
Objektif : Melindungi peralatan dan maklumat.		
050201 Perkakasan		
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:	Semua

	PERKARA	TANGGUNGJAWAB
	a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri - ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	
050202 Dokumen		
	Bagi memastikan integriti maklumat, langkah - langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c. Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang	Semua

	PERKARA	TANGGUNGJAWAB
	disediakan dan dihantar secara elektronik; dan d. Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	
050203 Media Storan		
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah - langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat : a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri - ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d. Pergerakan media storan hendaklah direkodkan.	Semua

PERKARA		TANGGUNGJAWAB
050204 Kabel		
	Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. 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; dan d. Hanya kakitangan dari Seksyen Teknologi Maklumat dibenarkan membuat sebarang pindaan atau penyelenggaraan.	STM dan ICTSO
050205 Penyelenggaraan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses	Semua

	PERKARA	TANGGUNGJAWAB
	penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Penolong Pengarah Seksyen Teknologi Maklumat.	
050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat		
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah - langkah berikut boleh diambil untuk menjamin keselamatan perkakasan : a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai yang bertanggungjawab dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
050207 Peralatan di Luar Premis		
	Bagi perkakasan yang dibawa keluar dari premis JAWHAR, langkah - langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan JAWHAR: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan	Semua

PERKARA		TANGGUNGJAWAB
	b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri - ciri keselamatan yang bersesuaian.	
050208 Pelupusan		
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JAWHAR: 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; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada 1PP KP 2.6/2016 (Tatacara Pengurusan Aset Alih Kerajaan : Pelupusan).	Semua
050209 *Clear Desk* dan *Clear Screen*		
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk*	Semua

PERKARA		TANGGUNGJAWAB
	bermaksud tidak meninggalkan bahan - bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya : a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; dan b. Bahan - bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	
Keselamatan Persekitaran		
Objektif: Melindungi aset ICT JAWHAR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan		
050301 Kawalan Persekitaran		
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik	Semua

PERKARA		TANGGUNGJAWAB
	percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; 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. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang - kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
050302 Bekalan Kuasa		
	a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan	STM, ICTSO

PERKARA		TANGGUNGJAWAB
	bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
050303 Prosedur Kecemasan		
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	Semua

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

PERKARA		TANGGUNGJAWAB
Pengurusan Prosedur Operasi		
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat		
060101 Pengendalian Prosedur		
	a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, 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
060102 Kawalan Perubahan		
	a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai	Semua

PERKARA		TANGGUNGJAWAB
	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 d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Prosedur Pengurusan Insiden		
	Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan - kawalan berikut: a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan	JPICT JAWHAR , ICTSO

PERKARA		TANGGUNGJAWAB
	mengaktifkan pelan kesinambungan perkhidmatan (jika perlu); c. Menyimpan jejak audit dan memelihara bahan bukti (jika perlu); dan d. Menyediakan tindakan pemulihan segera.	
Perancangan dan Penerimaan Sistem		
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan Sistem		
060201 Perancangan Kapasiti		
	a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri - ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT, ICTSO
060202 Penerimaan Sistem		
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah	Pentadbir Sistem ICT, ICTSO

PERKARA		TANGGUNGJAWAB
	memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	
Perisian Berbahaya		
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan		
060301 Perlindungan dari Perisian Berbahaya		
	a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus dan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemaskini *pattern* antivirus setiap minggu; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai	Semua

PERKARA		TANGGUNGJAWAB
	ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
Housekeeping		
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila - bila masa		
060401 Penduaan		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site*. a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang - kurangnya sekali atau setelah	Semua

PERKARA		TANGGUNGJAWAB
	mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	
060402 Sistem Log		
	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 tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	STM
Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan		
060501 Kawalan Infrastruktur Rangkaian		
	Infrastruktur Rangkaian mestilah dikawal dan	Pentadbir Rangkaian dan

	PERKARA	TANGGUNGJAWAB
	diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah - langkah yang perlu dipertimbangkan : 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 iaitu kakitangan dari seksyen sokongan dan operasi; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JAWHAR; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada	Pentadbir Sistem ICT

PERKARA		TANGGUNGJAWAB
	komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti - aktiviti lain yang boleh mengancam sistem dan maklumat JAWHAR; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan JAWHAR hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian JAWHAR sahaja. Penggunaan modem atau melakukan penyambungan ke rangkaian lain atau yang seumpamanya, adalah dilarang sama sekali; dan l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
Pengurusan Laman Web		
Objektif: Melindungi dan mengemaskini maklumat di dalam Laman Web		
060601 Laman Web		
	a. Proses pengurusan kandungan laman	STM

PERKARA		TANGGUNGJAWAB
	web/portal meliputi penulisan, semakan teks penulisan, semakan editorial serta penerbitan di laman web/portal perlu mendapat kelulusan pihak pengurusan; b. Penyelenggaraan dan penambahbaikan laman web perlu dilakukan secara berterusan bagi menjamin maklumat yang terdapat di laman web/portal adalah terkini dan sahih; c. Memastikan laman web/portal memenuhi tahap keselamatan yang ditetapkan bagi mengelakkan berlakunya pencerobohan; dan d. Memastikan kapasiti perkakasan dan perisian yang mencukupi untuk menampung operasi laman web/portal.	
Pengurusan Media		
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal		
060701 Penghantaran dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media		
	a. Melabelkan semua media mengikut tahap	Semua

	PERKARA	TANGGUNGJAWAB
	sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; 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 f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
060703 Keselamatan Sistem Dokumentasi		
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri - ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Pentadbir Sistem ICT, ICTSO

PERKARA		TANGGUNGJAWAB
Keselamatan Komunikasi		
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat		
060801 Internet		
	a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JAWHAR; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan papan buletin. Walau bagaimana pun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk	Semua

PERKARA		TANGGUNGJAWAB
	kepada dasar dan peraturan yang telah ditetapkan; dan g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	
060802 Mel Elektronik		
	a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh JAWHAR 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 JAWHAR; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk	Semua

	PERKARA	TANGGUNGJAWAB
	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; h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.	

PERKARA 07 KAWALAN CAPAIAN

PERKARA		TANGGUNGJAWAB
Dasar Kawalan Capaian		
Objektif : Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset JAWHAR		
070101 Keperluan Dasar		
	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.	STM, ICTSO
Pengurusan Capaian Pengguna		
Objektif : Mengawal capaian pengguna ke atas aset ICT JAWHAR		
070201 Akaun Pengguna		
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Akaun pengguna yang diwujudkan	Semua

PERKARA		TANGGUNGJAWAB
	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 jabatan. 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 dan menamatkan akaun pengguna atas sebab - sebab berikut: i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Ke agensi lain; iv. Bertukar; v. Bersara; atau vi. Ditamatkan perkhidmatan.	
070202 Jejak Audit		
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan	Pentadbir Sistem ICT

<table>
<tr><th colspan="2">PERKARA</th><th>TANGGUNGJAWAB</th></tr>
<tr><td></td><td>sistem. Aktiviti jejak audit mengandungi:

a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;
b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

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.</td><td></td></tr>
<tr><td colspan="3">Kawalan Capaian Sistem dan Aplikasi</td></tr>
<tr><td colspan="3">Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan</td></tr>
<tr><td colspan="3">070301 Sistem Maklumat dan Aplikasi</td></tr>
<tr><td></td><td>Capaian sistem dan aplikasi di JAWHAR</td><td>Pentadbir Sistem ICT,</td></tr>
</table>

	PERKARA	TANGGUNGJAWAB
	adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah - langkah berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti - aktiviti yang tidak diingini; c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri - ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	ICTSO

PERKARA		TANGGUNGJAWAB
Peralatan Komputer Mudah Alih		
Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih		
070401 Penggunaan Peralatan Komputer Mudah Alih		
	a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua

PERKARA 08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PERKARA		TANGGUNGJAWAB
Keselamatan Dalam Membangunkan Sistem dan Aplikasi		
Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian		
080101 Keperluan Keselamatan		
	a. Pembangunan 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; dan c. Sebaiknya - baiknya, 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, ICTSO

PERKARA		TANGGUNGJAWAB
Kriptografi		
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat		
080201 Penyulitan		
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Tandatangan Digital		
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
080203 Pengurusan Infrastruktur Kunci 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

PERKARA		TANGGUNGJAWAB
Fail Sistem		
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat		
080301 Kawalan Fail Sistem		
	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 aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
Pembangunan dan Proses Sokongan		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi		
080401 Kawalan Perubahan		
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah	Pentadbir Sistem ICT

PERKARA		TANGGUNGJAWAB
	dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	

PERKARA 09 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

<table>
<tr><th colspan="2">PERKARA</th><th>TANGGUNGJAWAB</th></tr>
<tr><td colspan="3">Dasar Kesinambungan Perkhidmatan</td></tr>
<tr><td colspan="3">Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan</td></tr>
<tr><td colspan="3">090101 Pelan Kesinambungan Perkhidmatan</td></tr>
<tr><td></td><td>Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian:

a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
b. Melaksanakan prosedur - prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
c. Mendokumentasikan proses dan prosedur yang telah dipersetujui;
d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
e. Membuat penduaan; dan
f. Menguji dan mengemaskini pelan</td><td>ICTSO</td></tr>
</table>

PERKARA		TANGGUNGJAWAB
	sekurang-kurangnya setahun sekali.	

PERKARA 10 PEMATUHAN

PERKARA		TANGGUNGJAWAB
Pematuhan dan Keperluan Perundangan		
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT JAWHAR		
100101 Pematuhan Dasar		
	Setiap pengguna di JAWHAR hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT JAWHAR dan undang - undang atau peraturan - peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di JAWHAR termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
100102 Keperluan Perundangan		
	Berikut adalah keperluan perundangan atau peraturan - peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JAWHAR: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi	Semua

	PERKARA	TANGGUNGJAWAB
	Kerajaan"; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi - agensi Kerajaan"; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Akta Tandatangan Digital 1997; h. Akta Jenayah Komputer 1997; i. Akta Hak cipta (Pindaan) Tahun 1997; dan j. Akta Komunikasi dan Multimedia 1998	

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT
JABATAN WAKAF, ZAKAT DAN HAJI (JAWHAR)

Nama (Huruf Besar) :…………………………………………………………………….

No. Kad Pengenalan :……………………………………………………………………

Jawatan :……………………………………………………………….

Bahagian :………………………………………………………………

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT Jabatan Wakaf, Zakat dan Haji (JAWHAR); dan

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

Tanda tangan :…………………………………..

Tarikh :…………………………………..

Pengesahan Pegawai Keselamatan ICT

……………………………………….
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Pengarah
Tarikh : ....