Kementerian Pertanian dan Industri Asas Tani (MOA)

Dasar Keselamatan ICT

Versi: 1.2

KANDUNGAN

TAKRIF ..... **II**

1. SEJARAH DOKUMEN **4**

1.1 **JADUAL PINDAAN DOKUMEN** **5**

2. BAHAGIAN I - PENGENALAN **7**

2.1 OBJEKTIF 7
2.2 SKOP 8
2.3 PRINSIP YANG PERLU DIIKUTI 9
2.4 PELANGGARAN DAN HUKUMAN 12
2.5 SEMAKAN DAN PENYELENGGARAAN DOKUMEN 13
2.6 RUJUKAN 13

3. BAHAGIAN II - DASAR **14**

01: PENGUATKUASAAN DAN PENYELENGGARAAN DASAR 14
02: ORGANISASI KESELAMATAN MAKLUMAT 15
03: PENGURUSAN ASET 21
04: KESELAMATAN SUMBER MANUSIA 23
05: KESELAMATAN FIZIKAL DAN PERSEKITARAN 26
06: PENGURUSAN KOMUNIKASI DAN OPERASI 30
07: KAWALAN CAPAIAN 37
08: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT 43
09: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 47
10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 49
11: PEMATUHAN 52
APPENDIK 58
APPENDIK A: SURAT AKAUN PEMATUHAN DASAR KESELAMATAN ICT MOA 59
APPENDIK B: MEDIA SANITISATION GUIDELINE 60
APPENDIK C: RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT AGENSI 73

TAKRIF

Aset ICT	Sebarang objek ICT yang mempunyai nilai kepada organisasi.
Backup	Salinan fail atau program yang dijanakan untuk memudahkan proses pemulihan dijalankan.
Business Impact Analysis	Analisa berkaitan keperluan sistem ICT, proses dan hubungankait antara keduanya yang digunakan untuk menyediakan sistem kontigensi dan keutamaan yang perlu diberikan semasa bencana.
Change Management	Proses yang memastikan semua perubahan ke atas infrastruktur ICT ditaksirkan, ditentusahkan, dilaksanakan dan dikaji semula dalam keadaan terkawal untuk memastikan gangguan tidak berlaku.
Dasar	Pernyataan peringkat tinggi mengenai prinsip, matlamat dan objektif termasuk juga cara-cara untuk mencapainya bagi subjek yang spesifik.
Emel	Mesej yang dihantar secara elektronik.
Impak	Hasil atau lanjutan dari sesuatu kejadian.
Integriti	Keadaan di mana maklumat tersimpan mengikut cara yang dibenarkan dan tiada perubahan dilakukan yang menjadikan maklumat itu berlainan dari asal.
Kawalan	Langkah-langkah penjagaan yang mana bila ia dilakukan dengan betul, akan mengurangkan risiko kemusnahan terhadap aset.
Kerahsiaan	Keadaan di mana maklumat sensitif dikawal dan diberikan kepada pengguna yang sah sahaja.

Keselamatan Fizikal	Prosedur kawalan yang wujud untuk menghalang penceroboh dari memasuki sistem atau prasarana.
Ketersediaan	Keadaan di mana maklumat atau proses sentiasa boleh dicapai dan digunakan oleh pihak yang dibenarkan.
Pengasingan Tugas	Pengasingan tugas dan tanggungjawab supaya tiada individu boleh mengsabotaj sistem kritikal yang dikendalikannya.
Pengguna ICT	Kakitangan MOA (Tetap, sementara, kontrak) atau pihak ketiga (perunding, kontraktor, pembekal dan pembekal perkhidmatan) yang diberikan hak capaian kepada aset ICT MOA.
Pihak Ketiga	Individu yang selain dari kakitangan MOA seperti perunding, pembekal, kontraktor, pembekal perkhidmatan dan sebagainya. Kakitangan dari Agensi Kerajaan selain dari MOA juga diklasifikasikan sebagai pihak ketiga.
Risiko	Kemungkinan untuk sesuatu terjadi yang boleh memberikan impak kepada objektifnya.
Secure Areas	Kawasan di mana MOA menempatkan aset ICT yang sensitif dan kritikal seperti Pusat Data atau bilik pejabat yang mengandungi maklumat yang sulit.
Shred	Cara-cara untuk ‘membersihkan’ media, dengan cara merincih atau menghancurkannya kepada bahagian yang kecil.
Virus	Kod yang ditulis dengan niat jahat untuk memusnah cara komputer bekerja tanpa kebenaran pengguna.
Vulnerability	Kelemahan dari segi prosedur, senibina, implementasi dan kawalan dalaman yang boleh dieksploitasi hingga mengakibatkan pelanggaran aspek keselamatan atau dasar keselamatan.

1. SEJARAH DOKUMEN

Versi	Penulis	Tarikh Ubah	Kelulusan	Tarikh Kuatkuasa
1.0	SCAN	30/11/2009	Mesyuarat JPICT 2/2010	21 April 2010
1.1	ICTSO	24/8/2011	Mesyuarat JPICT 1/2012	20 Januari 2012
1.2	ICTSO	10 Nov 2012	Mesyuarat JPICT 1/2013	18 Feb 2013

JADUAL PINDAAN DOKUMEN

TARIKH	VERSI	BUTIRAN PINDAAN
10 November 2012	1.2	Memasukkan Perkara 40201 : Tanggungjawab Pengurusan, m/s 24.
		Memasukkan Perkara 50105 : Kawalan Persekitaran, m/s 26.
		Memasukkan Perkara 50107 : Kawasan Akses Awam, Penghantaran dan Pemunggahan, m/s 27
		Memasukkan Perkara 50205 : Keselamatan Peralatan di Luar Premis, m/s 28
		Memasukkan Perkara 60402 : Perlindungan dari *Mobile Code*, m/s 32
		Memasukkan Perkara 60703 : Prosedur Pengendalian Maklumat, m/s 33
		Memasukkan Perkara 60704 : Keselamatan Dokumentasi Sistem, m/s 34
		Memasukkan Perkara 60801 : Polisi dan Prosedur Pertukaran Maklumat, m/s 34
		Memasukkan Perkara 60902 : Maklumat Umum, m/s 35
		Memasukkan Perkara 70101 : Dasar Kawalan Capaian, m/s 37
		Memasukkan Perkara 70303 : Pengenalan Peralatan Dalam Rangkaian, m/s 39
		Memasukkan Perkara 70602 : Kerja Jarak Jauh *(Teleworking)*, m/s 42
		Memasukkan Sub Bidang : Audit Sistem

		Maklumat beserta Objektif, m/s 57
		Memasukkan Perkara 110301 : Pematuhan Keperluan Audit, m/s 57

2. BAHAGIAN I - PENGENALAN

Kakitangan di Kementerian Pertanian dan Industri Asas Tani (MOA) mempunyai tanggungjawab bersama untuk melindungi Aset ICT dan dalam masa yang sama mengawal maklumat dan hak intelek yang dipunyai oleh MOA. Segala aset yang kritikal perlulah dikawal untuk mengurangkan sebarang impak yang boleh mengganggu perkhidmatan di MOA. Kawalan keselamatan ICT di MOA merupakan fungsi kritikal yang perlu diterapkan ke dalam semua operasi dan perkhidmatan MOA.

Dokumen Dasar Keselamatan ICT menghuraikan pendekatan kementerian ke atas keselamatan ICT dan ia menjadi penanda aras komitmen dari pihak pengurusan. Dokumen ini akan menjadi dokumen rujukan utama yang menjurus kepada pembinaan dokumen yang berkaitan dengannya (garis panduan, prosedur dan sebagainya).

2.1 OBJEKTIF

Dokumen ini menyediakan penyataan Dasar Keselamatan ICT yang perlu dipatuhi oleh kakitangan MOA. Ia bertujuan untuk:

a. Memberi kesedaran kepada kakitangan tentang risiko keselamatan ICT dan cara-cara mengendalikannya;

b. Menerangkan peranan dan tanggungjawab kakitangan terhadap aset ICT; dan

c. Memastikan kerahsiaan, integriti dan ketersediaan ke atas aset ICT.

2.2 SKOP

2.2.1 Apakah bentuk maklumat yang terikat dengan dasar ini?

Dokumen ini tergunapakai pada segala:

a. Jenis maklumat itu diwakili (tulisan, ucapan, elektronik dan segala bentuk yang ada);

b. Teknologi yang digunakan untuk mengendalikan maklumat tersebut (kabinet fail, mesin faks, computer);

c. Lokasi maklumat (di dalam pejabat, lokasi pelanggan, di dalam kapalterbang); dan

d. Kitarhayat maklumat (asal-usul maklumat, kemasukannya, pemprosesaan, pembahagian, penyimpanan dan pelupusan).

2.2.2 Siapakah yang perlu mematuhi dasar ini?

Dasar ini tergunapakai oleh keseluruhan pengguna aset ICT di MOA. Tiada pengecualian diberikan kepada sesiapapun. Kakitangan MOA yang bertaraf tetap, sementara atau kontrak adalah terikat dengan dasar ini. Dasar ini turut terpakai kepada kakitangan yang bekerja secara jauh *(remote)*. Dokumen ini juga perlu dibaca bersama-sama dengan arahan/pekeliling dari pihak berkuasa dari masa ke masa.

Dalam keadaan-keadaan tertentu yang seperti dihuraikan pada mana-mana penyataan dasar, pihak ketiga perlu menghormati segala penyataan yang terdapat di dalam dasar yang sedia ada.

Dokumen dasar ini tergunapakai oleh:

a. Kakitangan MOA, tetap, sementara atau kontrak; dan

b. Pihak ketiga seperti perunding, kontraktor, pembekal perkhidmatan, pembekal dan agensi lain yang bertukar maklumat dengan MOA.

Tindakan akan diambil mengikut lunas undang-undang untuk memastikan dasar ini diikut dan dihormati.

2.3 PRINSIP YANG PERLU DIIKUTI

Berikut merupakan prinsip-prinsip asas yang perlu diikuti:

a. Capaian atas dasar "perlu tahu"

Capaian penggunaan kepada aset ICT perlulah diberi atas kegunaan yang spesifik dan terhad kepada pengguna yang relevan sahaja. Ia bermaksud capaian hanya boleh diberi mengikut keperluan peranan dan fungsi kerja mereka sahaja.

b. Capaian yang minimum

Capaian pengguna perlulah diberi pada tahap yang minimum sahaja. Kebenaran diperlukan sebelum hak untuk mencipta, menyimpan, mengemaskini, mengubah dan memusnahkan maklumat boleh diberi. Hak capaian perlulah dikaji kembali dari masa ke masa berdasarkan tanggungjawab kerja kakitangan.

c. Accountability

Semua kakitangan adalah bertanggungjawab atas segala tindakan mereka kepada aset ICT di MOA.

d. Pembahagian Tugas

Tugas untuk mencipta, memusnah, mengemaskini, mengubah dan menentusahkan data perlulah diasingkan untuk menghalang dari capaian yang tidak sah dan mengawal aset ICT dari sebarang ralat, , kebocoran atau manipulasi maklumat.

e. Audit

Audit adalah tugas mengenalpasti insiden-insiden yang boleh mengancam keselamatan. Ini termasuklah mengendalikan segala rekod yang berkaitan dengan ukuran keselamatan. Dari itu, segala aset ICT perlu dipastikan boleh menghasil dan menyimpan log keselamatan dan jejak audit.

f. Pematuhan

Dasar Keselamatan ICT MOA perlulah dibaca, difahami dan dipatuhi untuk menghindarkan sebarang pelanggaran arahan yang boleh mengancam keselamatan ICT.

g. Pemulihan

Pemulihan sistem adalah penting untuk memastikan kesediaan dan kebolehcapaian pada setiap masa. Objektif utamanya adalah untuk meminimumkan kerosakan atau kerugian akibat dari ketiadaan perkhidmatan. Pemulihan boleh dihasilkan melalui salinan *(backup)* dan menyediakan pelan pemulihan bencana *(Disaster Recovery Plan)*.

h. Saling Bergantung

Semua prinsip-prinsip di atas adalah saling berkait dan saling melengkapi antara satu sama lain. Tugas untuk mengasingkan cara kerja dengan

menyusun dan mereka bentuk mekanisma keselamatan adalah penting untuk memastikan kawalan keselamatan yang maksimum.

2.4 PELANGGARAN DAN HUKUMAN

2.4.1 Pelanggaran

Sebarang pelanggaran dasar perlulah dilaporkan pada Bahagian Pengurusan Maklumat (BPM). Insiden perlulah disiasat oleh BPM, dengan kerjasama penyelia kakitangan terbabit dan pihak berkuasa yang berkaitan.

2.4.2 Tindakan Disiplin

Pelanggaran dasar secara sengaja akan menyebabkan:

a. Kehilangan hak capaian ke atas sumber maklumat;

b. Penilaian prestasi kerja yang buruk;

c. Dikenakan tindakan tatatertib;

d. Digantung kerja atau ditamatkan perkhidmatan;

e. Ditamatkan kontrak;

f. Dikenakan tindakan undang-undang.

2.5 SEMAKAN DAN PENYELENGGARAAN DOKUMEN

ICT Security Officer (ICTSO) [1] merupakan pemunya dokumen ini. Dia bertanggungjawab untuk menyemak dan menyelenggarakan dasar ini.

2.6 RUJUKAN

a. Information Security – Security techniques – Code of practice for information security management (ISO/IEC 17799 : 2005)

b. Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2005)

c. *Akta Arkib Negara 2003*

d. *Arahan Keselamatan*

e. *Arahan Teknologi Maklumat 2007 – MAMPU*

f. Guidelines for Media Sanitisation : The NIST Handbook (Special Publication 800-88)", United States : National Institute of Standards and Technology, 2006

g. Malaysian Public Sector Management Of ICT Security Handbook (MyMIS)

h. *Surat Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi*

i. *Surat Pekeliling Am Bil. 4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam*

[1] Senarai Tugas ICTSO

3. BAHAGIAN II – DASAR

01: PENGUATKUASAAN DAN PENYELENGGARAAN DASAR

Dasar Keselematan ICT		
Objektif	Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MOA dan perundangan yang berkaitan.	
010101	**Penguatkuasaan Dasar**	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha MOA dan dibantu oleh CIO, ICTSO & semua Setiausaha / Pengarah Bahagian.	KSU
010102	**Sebaran Dasar**	
	Dasar ini perlu difahami oleh pengguna ICT di MOA. Semua kakitangan di MOA perlu menandatangani borang Akuan Pematuhan Dasar Keselamatan ICT sebelum mencapai sebarang aset ICT di MOA. Sila rujuk pada Appendik A: Akuan Pematuhan Dasar Keselamatan ICT.	Semua
010103	**Penyelenggaraan Dasar**	
	Dasar ini perlu disemak setahun sekali dan dikemaskini berdasarkan perubahan yang diterima dari laporan penilaian risiko, insiden keselamatan, ancaman terkini dan juga perubahan ke atas infrastruktur di MOA. Semakan ini perlu disertakan sekali hasil penilaian terhadap keberkesanan dasar berdasarkan:	ICTSO

Dasar Keselematan ICT		
Objektif	Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MOA dan perundangan yang berkaitan.	
	a. Persekitaran dan jumlah impak yang direkodkan dari semua insiden keselamatan; b. Kos dan impak terhadap kawalan *(control)* yang berhubungkait dengan kecekapan bisnes; c. Kesan terhadap perubahan teknologi. Proses semakan dasar perlu meliputi: a. Mengenalpasti keperluan terhadap sebarang perubahan; b. Menghantar pelan perubahan bertulis kepada pihak pengurusan untuk proses semakan; c. Memberitahu akan perubahan yang dipersetujui kepada semua pengguna.	

02: ORGANISASI KESELAMATAN MAKLUMAT

Organisasi Dalaman		
Objektif	Menyatakan tugas dan tanggungjawab untuk semua individu di dalam pengurusan keselamatan ICT di dalam organisasi	
020101	**Ketua Setiausaha MOA**	
	Ketua Setiausaha MOA adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MOA; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MOA; (c) Memastikan semua keperluan organisasi (sumber	KSU

	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 MOA;	
020102	***Chief Information Officer (CIO)***	
	Chief Information Officer (CIO) bertanggungjawab: a. Menyediakan sumber untuk melaksanakan kawalan keselamatan ICT; b. Memantau keseluruhan prestasi dan kecekapan perkhidmatan keselamatan ICT; c. Mempersetujui dan menyokong semua inisiatif keselamatan; dan d. Menyemak dan mempersetujui Dasar Keselamatan ICT MOA.	CIO
020103	**Pengurus ICT**	
	Pengurus ICT MOA ialah Setiausaha Bahagian Bahagian Pengurusan Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MOA; b. Menentukan kawalan akses pengguna terhadap aset ICT MOA; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MOA.	Pengurus ICT

020104	ICT Security Officer (ICTSO)	
	ICTSO[2] bertanggungjawab untuk: a. Mengurus dan memantau keseluruhan program keselamatan ICT di MOA; b. Melaksanakan Dasar Keselamatan ICT; c. Memastikan kesemua pengguna ICT memahami dan mematuhi Dasar Keselamatan ICT dengan efektif melalui program kesedaran keselamatan di dalam organisasi; d. Membantu di dalam pembinaan garis panduan dan prosedur yang selari dengan Dasar Keselamatan ICT; e. Memastikan *Secure Areas* diberi perhatian penuh dan tindakan pantas perlu diambil dalam mengendalikannya. f. Menyediakan amaran awal tentang ancaman keselamatan ICT yang boleh membahayakan aset ICT MOA seperti ancaman virus yang terkini; g. Bekerjasama dengan pihak-pihak tertentu dalam menentukan masalah akar umbi berkaitan dengan insiden keselamatan, juga ancamannya serta cara untuk menyelamatkannya secepat mungkin; h. Melaporkan sebarang insiden keselamatan ICT kepada *Government Computer Emergency Response Team* (GCERT) dan memaklumkan kepada CIO; i. Menyediakan dokumen infrastruktur keselamatan ICT untuk kegunaan audit keselamatan; dan j. Menjalankan penilaian risiko *(risk assessment)*.	ICTSO

[2] *Senarai Tugas ICTSO*

020105	Jawatankuasa Keselamatan ICT	
	Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MOA. Di MOA, Jawatankuasa Pemandu ICT (JPICT) juga berperanan sebagai JKICT MOA. Keanggotaan JKICT MOA adalah seperti berikut: **Pengerusi :** CIO Kementerian **Ahli :** (1) CIO Jabatan / Agensi (2) Pengurus ICT Jabatan / Agensi (3) Semua Setiausaha / Pengarah Bahagian (4) ICTSO **Urus Setia** bagi JKICT MOA ialah urus setia yang mengendalikan JPICT. **Bidang kuasa:** (a) Memperakukan/meluluskan dokumen DKICT MOA; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MOA yang mematuhi keperluan DKICT MOA; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan DKICT MOA selaras dengan dasar-dasar ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran DKICT MOA; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	Jawatankuasa Keselamatan ICT

020106	***Bahagian Pengurusan Maklumat* (BPM)**	
	BPM bertanggungjawab untuk: a. Memastikan keselamatan semua konfigurasi bagi aset ICT; b. Mengambil tindakan yang pantas bila dimaklumkan mengenai: i. Pengguna ICT MOA yang ingin mengambil cuti panjang, dipindahkan kepada unit lain atau ditamatkan perkhidmatannya ii. Pihak ketiga yang telah menyelesaikan projek mereka atau ditamatkan perkhidmatannya oleh MOA. c. Memantau aktiviti capaian pengguna; d. Memastikan aktiviti luar biasa seperti pengubahan data yang tidak diluluskan dan melaporkan kepada ICTSO secepat mungkin untuk tindakan lanjut; e. Menghantar laporan capaian pengguna kepada pemilik maklumat dalam tempoh yang ditetapkan; dan f. Menyimpan dan menganalisa rekod audit.	BPM
020107	**Pengguna ICT**	
	Pengguna aset ICT bertanggungjawab untuk: a. Memahami implikasi keselamatan ICT atas tindakan mereka; b. Membaca, memahami dan mematuhi dasar keselamatan ICT dan mengawal aset ICT MOA; dan c. Melaporkan sebarang aktiviti yang boleh menjejaskan keselamatan ICT kepada BPM secepat mungkin.	Semua

Pihak Luaran		
Objektif	Untuk menjamin keselamatan maklumat MOA dan aset ICT yang dicapai, diproses dan disampaikan kepada atau diselenggarakan oleh pihak luaran.	
020201	**Pengenalpastian risiko berkaitan pihak luaran**	
	Bila wujud sebarang keperluan untuk pihak luaran mencapai aset atau maklumat ICT MOA, penilaian risiko perlu dilaksanakan terhadap mereka.	BPM
020203	**Menyertakan elemen keselamatan dalam Perjanjian dengan Pihak Ketiga**	
	Keperluan keselamatan ICT mestilah diambil kira dengan menyeluruh di dalam perjanjian dengan Pihak Ketiga sebelum mereka dibenarkan mencapai aset ICT MOA. Berikut adalah butiran yang perlu ada di dalam perjanjian tersebut: a. Dasar Keselamatan ICT MOA (bahagian yang tertentu sahaja); b. Tapisan Keselamatan; c. *Official Secrets Act 1972;*	BPM

03: PENGURUSAN ASET

Tanggungjawab Kepada Aset		
Objektif	Untuk mencapai dan memelihara perlindungan kepada aset ICT MOA.	
030101	**Inventori untuk aset ICT**	
	Inventori bagi aset ICT perlu diwujudkan. Setiap aset perlu direkodkan dan ditentukan pemiliknya. Ia juga perlu diberikan klasifikasi keselamatan yang dipersetujui dan didokumenkan.	Pemunya aset
030102	**Penggunaan aset ICT yang dibenarkan**	
	Semua pengguna mesti mengikut Dasar Penggunaan Yang Dibenarkan bagi mengendalikan aset.	Semua
Klasifikasi dan Pengendalian Maklumat		
Objektif	Untuk memastikan maklumat yang diterima dilindungi secara berpatutan.	
030201	**Klasifikasi Maklumat**	
	Maklumat perlu diklasifikasi dalam bentuk nilai, keperluan undang-undang, tahap sensitiviti dan kritikalnya kepada MOA.	Pemunya aset
030202	**Pengendalian Maklumat**	
	Pengendalian maklumat dalam sebarang bentuk bergantung kepada klasifikasi maklumat diberikan oleh pemunya aset.	Semua

Dokumen Berkaitan	Sila rujuk kepada topik berikut untuk penyataan dasar yang spesifik: a. Dasar Penggunaan yang Dibenarkan b. Dasar Klasifikasi dan Pengendalian Maklumat c. Dasar Keselamatan Operasi

04: KESELAMATAN SUMBER MANUSIA

Sebelum Diterima Bekerja		
Objektif	Untuk memastikan kakitangan, kontraktor dan pihak ketiga memahami tanggungjawab dan peranan mereka untuk mengurangkan risiko kecurian, penipuan dan salahguna peralatan.	
040101	**Keselamatan di dalam Tanggungjawab Kerja**	
	Peranan dan tanggungjawab keselamatan perlulah didokumenkan sebagai sebahagian dari tanggungjawab kerja.	*Cawangan Pengurusan Sumber Manusia*
040102	**Penyaringan**	
	Semua kakitangan MOA, kontraktor dan pihak ketiga mestilah disaring (untuk tugas sensitif) selari dengan undang-undang dan ketetapan yang digunapakai.	Semua
040103	**Terma dan Syarat Pelantikan**	
	Semua kakitangan MOA, kontraktor dan pihak ketiga mesti mematuhi terma dan syarat kontrak pelantikan yang menyatakan tanggungjawab mereka terhadap keselamatan ICT dan juga terhadap sebarang undang-undang dan ketetapan dari pihak berwajib. Semua kakitangan MOA, kontraktor dan pihak ketiga yang perlu kepada capaian maklumat sensitif, mestilah menandatangani dokumen *Non Disclosure Agreement (NDA)* terlebih dahulu.	Semua

Semasa Bekerja		
Objektif	Untuk memastikan semua kakitangan MOA, kontraktor dan pihak ketiga sedar akan ancaman keselamatan maklumat dan tanggungjawab melindunginya. , Mereka juga akan bertanggungjawab untuk menyokong dasar organisasi di dalam tugas harian bagi mengurangkan risiko kesilapan.	
040201	**Tanggungjawab Pengurusan**	
	Pihak pengurusan perlu memastikan setiap pengguna ICT, pembekal, perunding dan pihak-pihak lain yang berkepentingan memberikan perkhidmatan dan menguruskan keselamatan aset ICT berdasarkan perundangan dan peraturan didalam dasar, polisi, prosedur dan panduan yang telah ditetapkan oleh MOA.	
040202	**Kesedaran Keselamatan ICT, Pendidikan dan Latihan**	
	Semua pengguna ICT perlu diberikan kesedaran keselamatan yang mencukupi dan dimaklumkan mengenai perubahan dasar dan prosedur organisasi yang berkaitan dengan fungsi kerja mereka. ICTSO bertanggungjawab untuk merancang dan mengukur keberkesanan latihan dan juga bahan program keselamatan ICT yang diberikan dengan dibantu oleh Cawangan Pengurusan Sumber Manusia.	ICTSO, *Cawangan Pengurusan Sumber Manusia*
040203	**Tindakan Tatatertib**	
	Tindakan tatatertib yang formal akan dilaksanakan terhadap sesiapa yang melanggar peraturan keselamatan. Rujuk pada Seksyen 2.4 untuk penerangan lanjut.	Lembaga Tatatertib
Penamatan atau Perubahan Tugas		
Objektif	Untuk memastikan kakitangan, kontraktor dan pihak ketiga yang keluar atau	

	ditukarkan dari MOA, diurus dengan teratur.	
040301	**Tindakan Berkaitan Penamatan atau Perubahan Tugas**	
	Dalam keadaan seseorang kakitangan ditukarkan atau diberhentikan tugas dari MOA, Cawangan Pengurusan Sumber Manusia bertanggungjawab untuk memberitahu bahagian yang berkaitan supaya ia dapat memastikan: a. Harta kepunyaan MOA yang dipegang oleh kakitangan tersebut diserahkan kembali sebelum mereka tamat perkhidmatan; b. Akaun capaian komputer dan komunikasi yang digunakan oleh kakitangan tersebut dipotong/digantung; c. Sebarang hak istimewa ditamat/dipotong; d. Semua capaian fizikal/logikal mestilah diputuskan dan ditukar; dan e. Semua maklumat yang berkaitan dengan organisasi dikembalikan kepada MOA sebelum mereka beredar pergi. Semua kontraktor dan pihak ketiga mestilah mengembalikan semua aset MOA yang masih dalam pegangan mereka sebelum perjanjian ditamatkan.	Semua

05: KESELAMATAN FIZIKAL DAN PERSEKITARAN

Secure Areas		
Objektif	Menghalang capaian fizikal tanpa kebenaran, kemusnahan dan ganggu gugat kepada maklumat dan premis organisasi.	
050101	**Perimeter Keselamatan Fizikal**	
	Semua lokasi yang menempatkan aset ICT MOA perlulah dikawal secara fizikal selari dengan kepentingan fungsinya.	Semua
050102	**Kawalan Kemasukan Fizikal**	
	Capaian ke atas *Secure Areas* mestilah di hadkan secara fizikal kepada kakitangan yang dibenarkan sahaja.	Semua
050103	**Pas Kerja / Pas Pelawat**	
	Semua individu perlu memakai Pas Kerja / Pas Pelawat pada pakaian mereka dan ia mestilah boleh dilihat dengan jelas ketika berada di dalam premis MOA.	Semua
050104	**Pengendalian Pelawat dan Pihak Ketiga**	
	Semua pelawat dan pihak ketiga yang memasuki *Secure Areas* perlulah diawasi dan diiringi. Mereka hanya dibenarkan masuk atas urusan rasmi sahaja.	Semua
050105	**Kawalan Persekitaran**	
	Semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian	Semua

	hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan MOA bagi mencegah kerosakan dan gangguan terhadap premis dan aset ICT MOA. Perlindungan fizikal terhadap kerosakan akibat kebakaran, banjir, gempa bumi, letupan, rusuhan awam, dan lain-lain bentuk bencana alam atau buatan manusia mesti dibangun dan digunakan.	
050106	**Pengawasan *Secure Areas***	
	Semua *Secure Areas* perlulah dikunci dan dikawal oleh CCTV pada setiap masa.	BPM
050107	**Kawasan Akses Awam, Penghantaran dan Pemunggahan**	
	Semua akses kepada premis MOA mesti dikawal, dipantau dan diasingkan daripada kemudahan pemprosesan maklumat untuk menghalang capaian yang tidak dibenarkan	MOA
	Keselamatan Peralatan	
Objektif	Menghalang kehilangan, kerosakan atau kecurian ke atas aset, yang menyebabkan gangguan kepada aktiviti MOA.	
050201	**Kawalan Peralatan**	
	Alatan mestilah ditempatkan dan dilindungi dengan betul untuk mengurangkan risiko ke atas ancaman persekitaran, bahaya dan peluang untuk capaian tanpa kebenaran.	BPM
050202	**Utiliti Sokongan**	
	Peralatan mestilah dilindungi dari kegagalan kuasa elektrik dan sebarang gangguan yang disebabkan oleh kegagalan utiliti sokongan.	BPM

050203	**Keselamatan Pengkabelan**	
	Kabel kuasa dan telekomunikasi yang membawa data atau sebarang maklumat mestilah dilindungi dari pintasan dan kerosakan.	BPM
050204	**Penyelenggaraan Peralatan**	
	Semua alatan mestilah diselenggara secara berkala dan sebarang proses pembaikan hendaklah dilaksanakan oleh pihak yang berkelayakan sahaja.	BPM
050205	**Keselamatan Peralatan di Luar Premis**	
	MOA mestilah memastikan bahawa akses kepada kemudahan pemprosesan maklumat di luar premis dimana data disimpan dikawal dan hanya diberikan kepada kakitangan yang dibenarkan. Peralatan ICT yang dibawa keluar dari premis MOA adalah terdedah kepada pelbagai risiko maka semua dasar, polisi, prosedur dan panduan keselamatan berkaitan yang ditetapkan terpakai keatasnya.	BPM
050206	**Pelupusan Selamat atau Penggunaan Semula Peralatan**	
	Semua peralatan yang mengandungi media storan mestilah diperiksa untuk memastikan sebarang maklumat sensitif dan perisian berlesen telah dimusnahkan sebelum proses pelupusan. Sila rujuk kepada Appendik B: *Media Sanitisation Guideline* dan Arahan Teknologi Maklumat. Barangan seperti katrij inkjet, toner laser mestilah dilupuskan pada persekitaran yang sesuai sepertimana yang disyorkan oleh pihak pembekal.	Semua
050207	**Pelupusan Barangan Milik MOA**	
	Peralatan, maklumat atau perisian hendaklah	Lembaga

	disahkan sebelum dibawa keluar.	Pemeriksa Aset
Dokumen Berkaitan	Sila rujuk kepada topik berikut untuk penyataan dasar yang spesifik: a. Dasar Keselamatan Fizikal	

06: PENGURUSAN KOMUNIKASI DAN OPERASI

Prosedur Operasi dan Tanggungjawab		
Objektif	Memastikan operasi yang betul dan selamat untuk aset ICT MOA.	
060101	**Dokumentasi Prosedur Operasi**	
	Semua prosedur yang berkaitan dengan operasi fungsi komputer mestilah didokumenkan secara lengkap dan dipatuhi perlaksanaannya. Penyelenggaraan secara berkala perlu untuk memastikan operasi ICT MOA ditangani efisien dan konsisten.	BPM
060102	***Change Management***	
	Sistem pengoperasian komputer dan perisian mestilah mengikuti proses *Change Management* yang betul.	BPM
060103	**Pembahagian Tugas**	
	Tugas dan tanggungjawab mestilah dibahagikan untuk mengurangkan risiko salahguna kuasa, salahguna aset atau perubahan tanpa sengaja terhadap aset ICT MOA.	Semua
Penyampaian Perkhidmatan oleh Pihak Ketiga		
Objektif	Memastikan perkhidmatan yang diberi mempunyai tahap keselamatan ICT yang bersesuaian selari dengan kontrak perjanjian.	
060201	**Penyampaian Perkhidmatan**	

	Kawalan keselamatan, takrif perkhidmatan dan tahap kualiti penghantaran perkhidmatan mestilah terdapat dalam semua perjanjian yang berkaitan.	Semua
060202	**Memantau dan Menilai Perkhidmatan Pihak Ketiga**	
	Semua perkhidmatan beserta laporan dan rekod yang diberi oleh pihak ketiga perlulah dipantau dan dinilai.	Semua
060203	**Mengurus Perubahan Skop Perkhidmatan Oleh Pihak Ketiga**	
	Sebarang perubahan skop perkhidmatan yang berikan oleh pihak ketiga mestilah diurus. Ia termasuklah bekalan, perubahan terhadap perkhidmatan sedia ada dan pertambahan perkhidmatan baru. Penilaian risiko perlu dilakukan berdasarkan tahap kritikal sesebuah sistem dan impak yang ada terhadap perubahan ini.	Semua
Perancangan dan Penerimaan Sistem		
Objektif	Meminimakan risiko terhadap kegagalan sistem.	
060301	**Pengurusan Kapasiti**	
	Penggunaan sumber mestilah dipantau dan diperbaiki. Pelan masa hadapan mestilah dibina terhadap keperluan kapasiti untuk memastikan kelancaran prestasi sistem.	BPM
060302	**Penerimaan Sistem**	
	Kriteria penerimaan untuk sistem ICT baru, penambahbaikan, dan versi terkini mestilah ditetapkan. Pemeriksaan yang sesuai mestilah dijalankan semasa pembinaan dan sebelum penerimaan sistem.	Pemunya Sistem

Pengawalan dari Perisian Berisiko *(Malicious Software)*		
Objektif	Melindungi integriti maklumat dan perisian	
060401	**Kawalan Ke Atas Perisian Berisiko**	
	Kawalan berkaitan pengecaman, pencegahan dan pemulihan terhadap perisian berisiko dan program kesedaran terhadap pengguna mestilah dijalankan.	BPM
060402	**Perlindungan dari *Mobile Code***	
	Penggunaan *mobile code* perlu mendapat kebenaran dan konfigurasi *mobile code* perlu dipastikan supaya beroperasi mengikut dasar, polisi, prosedur dan panduan keselamatan ICT MOA	BPM
Backup		
Objektif	Memastikan integriti dan ketersediaan aset ICT	
060501	**Salinan Maklumat *(Information Backup)***	
	Salinan maklumat dan perisian mestilah dilakukan dan diperiksa secara berkala.	BPM
Pengurusan Keselamatan Rangkaian		
Objektif	Memastikan perlindungan ke atas maklumat dan infrastruktur rangkaian	
060601	**Kawalan Rangkaian**	
	Rangkaian MOA mestilah dikendalikan dan diselenggara untuk memastikan ianya dipelihara daripada sebarang ancaman demi memantapkan keselamatan sistem dan aplikasi yang menggunakan rangkaian. Kawalan juga perlu difokuskan ke atas maklumat yang melalui rangkaian tersebut.	BPM

060602	**Keselamatan Perkhidmatan Rangkaian**	
	Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi keseluruhan perkhidmatan rangkaian MOA mestilah dikenalpasti dan disertakan ke dalam sebarang perjanjian yang berkaitan dengannya.	BPM
	Pengendalian Media	
Objektif	Menghalang sebarang pendedahan, perubahan, pengalihan dan pemusnahan aset dan gangguan ke atas aktiviti MOA.	
060701	**Pengurusan Media**	
	Semua prosedur dan tahap pengesahan untuk pengurusan media mestilah didokumenkan secara jelas.	BPM
060702	**Pelupusan Media**	
	Media yang mengandungi maklumat sensitif mestilah dihapuskan secara selamat dan betul. Cara-cara tersebut terdapat di Appendik B: *Media Sanitisation Guideline* dan Arahan Teknologi Maklumat.	Semua
060703	**Prosedur Pengendalian Maklumat**	
	Prosedur untuk pengendalian dan penyimpanan maklumat perlu diwujudkan untuk melindungi maklumat milik MOA daripada pendedahan tanpa kebenaran atau penyalahgunaan.	Semua

060704	**Keselamatan Dokumentasi Sistem**	
	Dokumentasi sistem perlu dilindungi dengan kawalan keselamatan yang secukupnya untuk mencegah capaian yang tidak dibenarkan.	BPM
	Pertukaran Maklumat	
Objektif	Mengekalkan keselamatan pertukaran maklumat dan perisian di MOA atau dengan pihak luaran	
060801	**Polisi dan Prosedur Pertukaran Maklumat**	
	Dasar, polisi, prosedur, dan kawalan perlu dibangunkan bertujuan melindungi pertukaran maklumat melalui penggunaan semua jenis kemudahan komunikasi di MOA	Semua
060802	**Perjanjian Pertukaran**	
	Perjanjian mesti diwujudkan untuk pertukaran maklumat (elektronik atau cetakan) dan perisian antara MOA dan pihak luaran bergantung kepada tahap sensitif sesuatu maklumat yang dikendalikan.	Semua
060803	**Media Fizikal semasa transit**	
	Media yang mengandungi maklumat mestilah dikawal dari capaian tanpa kebenaran, salahguna dan binasa semasa proses transit keluar dari premis MOA.	Semua
	Emel	
Objektif	Memastikan maklumat elektronik dan infrastruktur sokongan dikawal dan dilindungi	
060901	**Penggunaan yang dibenarkan**	

	Emel MOA hanya boleh digunakan untuk aktiviti kerja harian. Penggunaan untuk kepentingan peribadi adalah terlarang. Sila rujuk Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-Agensi Kerajaan *dan* Dasar Penggunaan Yang Dibenarkan.	Semua
060902	**Maklumat Umum**	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut : a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem yang boleh di akses oleh orang awam di uji terlebih dahulu; dan b. Melindungi integriti maklumat yang diberikan pada orang awam daripada pengubahsuaian yang tidak dibenarkan dan penyalahgunaan.	Semua
	Pemantauan	
Objektif	Mengesan sebarang aktiviti pemprosesan maklumat tanpa kebenaran	
061001	**Pemantauan Sistem Yang Digunakan**	
	Penggunaan aset ICT mestilah dipantau untuk mengesan sebarang aktiviti tanpa kebenaran dan memastikan pengguna hanya melaksanakan fungsi yang dibenarkan sahaja.	BPM
061002	**Penyimpanan Log**	
	Log mestilah dihasilkan dan disimpan berdasarkan tempoh yang terkandung di dalam ***Arahan Teknologi Maklumat*** dan Akta Arkib Negara 2003. Ini akan digunakan untuk membantu proses siasatan dan pemantauan kawalan capaian pada masa	BPM

	hadapan. Kemudahan penyimpanan log dan maklumatnya mestilah dikawal dari sebarang capaian tanpa kebenaran. Sebarang ralat yang dilaporkan oleh pengguna atau sistem perlulah disimpan. Log yang disimpan itu mestilah dianalisa untuk membenarkan proses tindakan susulan boleh dilaksanakan.	
061003	**Penyamaan Masa *(Clock Synchronization)***	
	Masa yang berkaitan dengan sistem ICT MOA mestilah disamakan dengan punca masa yang tepat. Ini untuk memastikan ketepatan masa log yang disimpan dan mengawal integriti log tersebut untuk kegunaan masa hadapan.	BPM
Dokumen Berkaitan	Sila rujuk kepada topik berikut untuk penyataan dasar yang spesifik: a. Dasar Penggunaan Yang Dibenarkan b. Dasar Keselamatan Rangkaian c. Dasar Keselamatan Operasi d. Dasar Keselamatan Fizikal e. Dasar Keselamatan Sistem	

07: KAWALAN CAPAIAN

Pengurusan Capaian Pengguna		
Objektif	Memastikan capaian pengguna yang dibenarkan dan untuk menghalang capaian tanpa kebenaran ke atas aset ICT.	
070101	**Dasar Kawalan Capaian**	
	Bertujuan mengawal capaian ke atas maklumat, kemudahan-kemudahan proses maklumat, dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira penyebaran dan pengesahan maklumat. 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. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	Semua

070102	**Pendaftaran / Nyah Daftar Pengguna**	
	Satu prosedur formal berkaitan pendaftaran/nyahdaftar mestilah diwujudkan untuk memberi atau mengambil kembali capaian ke atas segala sistem dan perkhidmatan ICT MOA.	BPM
070103	**Pengurusan Keistimewaan *(Privilege Management)***	
	Pemberian hak keistimewaan kepada semua pengguna perlulah dihadkan dan dikawal.	BPM
070104	**Pengurusan Kata Laluan Pengguna**	
	Pemberian kata laluan mestilah dikawal melalui proses pengurusan yang rasmi dan merujuk kepada Polisi Katalaluan.	BPM
070105	**Semakan Hak Capaian Pengguna**	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	BPM
	Tanggungjawab Pengguna	
Objektif	Menghalang capaian tanpa kebenaran oleh pengguna dan kecurian atas maklumat dan aset ICT MOA.	
070201	**Penggunaan Kata Laluan**	
	Setiap pengguna ICT bertanggungjawab ke atas penggunaan dan pengawalan kata laluan yang mereka gunakan.	Semua
070202	**Peralatan Pengguna yang Tidak Diawasi *(Unattended)***	
	Pengguna mestilah memastikan peralatan yang	Semua

	berada dalam jagaan mereka dilindungi secukupnya.	
070203	***Clear Desk* dan *Clear Screen***	
	Maklumat berbentuk cetakan yang sensitif dan kritikal perlulah disimpan dengan betul bila tidak digunakan. Komputer perlulah dikunci dengan kata laluan ataupun keluar dari sistem bila dibiarkan tanpa pengawasan.	Semua
Kawalan Capaian Rangkaian		
Objektif	Menghalang capaian tanpa kebenaran ke atas perkhidmatan rangkaian	
070301	**Penggunaan Perkhidmatan Rangkaian**	
	Pengguna ICT mesti diberikan capaian kepada perkhidmatan yang dibenarkan sahaja.	Semua
070302	**Pengesahan Pengguna untuk Sambungan Luaran *(External Connection)***	
	Cara pengesahan yang betul mestilah digunakan untuk mengawal capaian oleh pengguna jarak jauh *(remote user)*.	BPM
070303	**Pengenalan Peralatan Dalam Rangkaian**	
	MOA perlu mempertimbangkan untuk menggunakan mekanisme pengesan peralatan secara automatik untuk mengesahkan sambungan daripada lokasi dan peralatan tertentu.	BPM
070304	**Diagnostik Jarak Jauh *(Remote Diagnostic)* dan Kawalan Port Konfigurasi**	
	Capaian fizikal dan logikal ke atas port diagnostik dan konfigurasi perlulah dikawal.	BPM

070305	**Pengasingan Rangkaian**	
	Kumpulan maklumat, perkhidmatan, pengguna dan sistem maklumat mestilah diasingkan di dalam rangkaian.	BPM
070306	**Kawalan Hubungan Rangkaian**	
	Semua rangkaian yang dikongsi *(shared networks)*, terutama sekali yang keluar daripada batasan MOA, kawalan mesti dilengkapkan untuk menghad capaian oleh pengguna yang ada.	BPM
	Kawalan Capaian Pengoperasian Sistem	
Objektif	Menghalang capaian tanpa kebenaran kepada sistem pengoperasian	
070401	**Kemasukan Selamat *(Secure Log-on)***	
	Capaian ke atas pengoperasian sistem mestilah dikawal melalui proses kemasukan selamat *(Secure Log-on)*.	BPM
070402	**Proses Identifikasi dan Pengesahan Pengguna**	
	Pengguna ICT mesti mempunyai *User ID* untuk kegunaan peribadi sahaja dan teknik pengesahan yang pragmatik mesti ada untuk mengesahkan identiti pengguna tersebut.	BPM
070403	**Sistem Pengurusan Kata Laluan**	
	Sistem yang digunakan untuk mengurus kata laluan mestilah berbentuk interaktif dan boleh memastikan kebolehan untuk mengsyorkan kata laluan yang berkualiti.	BPM
070404	**Penggunaan Sistem Utiliti**	

	Pengguna sistem utiliti yang berupaya melepasi kawalan sistem dan aplikasi mestilah dihadkan dan dikawal secara teliti.	BPM
070405	**Tamat Masa Sesuatu Sesi**	
	Sesi yang tidak aktif mestilah ditutup selepas satu tempoh yang telah ditetapkan. Masa Tamat *(time-out)* yang ditetapkan perlulah disokong oleh risiko keselamatan kawasan tersebut, klasifikasi maklumat yang dikendalikan dan aplikasi yang digunakan termasuk juga risiko yang berhubungan dengan penggunanya.	BPM
070406	**Had Masa Hubungan *(Connection Time)***	
	Batasan masa terhadap sesuatu hubungan mestilah digunakan untuk memberi kawalan keselamatan tambahan pada aplikasi berisiko tinggi.	BPM
Kawalan Capaian Untuk Aplikasi dan Maklumat		
Objektif	Menghalang capaian tanpa kebenaran ke atas maklumat yang berada di dalam sistem aplikasi	
070501	**Menghadkan Capaian Maklumat**	
	Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna mestilah dikawal.	BPM
070502	**Pengasingan Sistem yang Sensitif**	
	Sistem yang sensitif mestilah mempunyai persekitaran yang diasingkan dari sistem yang lain.	BPM
Pengkomputeran Mobil		
Objektif	Memastikan keselamatan maklumat semasa menggunakan	

	pengkomputeran mobil.	
070601	**Pengkomputeran Mobil dan Komunikasi**	
	Langkah-langkah keselamatan yang berpatutan perlu diambil untuk mengawalnya dari sebarang risiko semasa menggunakan pengkomputeran mobil dan kemudahan komunikasi.	Semua
070602	**Kerja Jarak Jauh *(Teleworking)***	
	Kawalan perlindungan dan keselamatan hendaklah diambil semasa kerja jarak jauh bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua
Dokumen Berkaitan	Sila rujuk kepada topik berikut untuk penyataan dasar yang spesifik: a. Dasar Penggunaan Yang Dibenarkan b. Dasar Pengkomputeran Mobil c. Dasar Keselamatan Rangkaian d. Dasar Keselamatan Operasi e. Dasar Kata laluan f. Dasar Keselamatan Sistem	

08: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Keperluan Keselamatan Sistem Maklumat		
Objektif	Memastikan keselamatan untuk semua sistem ICT	
080101	**Analisa dan Spesifikasi Keperluan Keselamatan**	
	Keperluan keselamatan mesti dikenal pasti dan dipersetujui sebelum sebarang pembinaan, perlaksanaan dan penambahbaikan sistem ICT dilakukan.	BPM
Pemprosesan yang Betul di dalam semua Aplikasi		
Objektif	Menghalang ralat, kehilangan, pengubahan dan penyalahgunaan maklumat di dalam aplikasi	
080201	**Kawalan di dalam Sistem Aplikasi**	
	Kawalan yang berpatutan dan backup log mestilah dibina ke dalam sistem aplikasi. Ini termasuk proses menentusahkan data input, proses luaran, pengesahan mesej, data output dan sebagainya.	BPM
080202	**Manual dan Dokumen Prosedur**	
	Semua prosedur, manual pengguna, dokumentasi sistem, pelan pemulihan dan pelan pengujian mestilah diwujudkan secara rasmi dan diselenggara dengan betul.	BPM
Kawalan Kriptografi		

Objektif	Mengawal kerahsiaan, kebenaran atau integriti maklumat dengan menggunakan cara kripto	
080301	**Penggunaan Kawalan Kriptografi**	
	Semua maklumat yang sensitif mestilah dikawal menggunakan kawalan kriptografi yang berlandaskan Dasar Keselamatan Sistem dan Dasar Klasifikasi dan Pengendalian Maklumat. Kunci enkripsi mestilah dilindungi dengan menggunakan cara kawalan yang terbaik dan hendaklah dirahsiakan.	Semua
080302	**Pengurusan Kunci**	
	Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.	BPM
	Keselamatan Fail Sistem	
Objektif	Memastikan keselamatan fail sistem	
080401	**Kawalan Perisian Operasi**	
	Prosedur mestilah wujud untuk mengawal proses instalasi perisian di dalam sistem yang sedang beroperasi untuk mengurangkan risiko kerosakan *(corruption).*	BPM
080402	**Kawalan Data Ujian bagi Sistem**	
	Ujian mesti dilakukan secara teliti, dikawal dan dilindungi.	BPM
080403	**Kawalan Capaian kepada Kod Sumber Program**	
	Capaian kepada kod sumber program mestilah	BPM

	dihadkan.	
Keselamatan di dalam Proses Pembinaan dan Sokongan		
Objektif	Memastikan keselamatan perisian sistem aplikasi dan maklumat	
080501	**Kawalan Perubahan *(Change Control)***	
	Sebarang perubahan mestilah dikawal oleh prosedur kawalan perubahan *(Change Control)* yang rasmi.	BPM
080502	**Semakan Teknikal bagi Aplikasi setelah Pengoperasian Sistem Ditukar**	
	Apabila pengoperasian sistem ditukar, aplikasi yang kritikal mesti disemak dan diuji untuk memastikan tiada kesan sampingan terhadap keselamatan dan operasi MOA akan berlaku.	BPM
080503	**Pembocoran Maklumat**	
	Sebarang peluang untuk membocorkan maklumat melalui apa sekali cara pun mestilah dihalang.	BPM
080504	**Pembinaan Perisian secara *'Outsource'***	
	Pembinaan perisian secara 'outsource' mestilah diselenggara dan dipantau.	BPM
Pengurusan *'Vulnerability'* Teknikal		
Objektif	Mengurangkan risiko yang dihasilkan oleh eksploitasi dari sebarang '*vulnerability'* teknikal	
080601	**Kawalan Terhadap *'Vulnerability'* Teknikal**	
	Sebarang maklumat yang berkaitan *'vulnerability'* teknikal bagi sistem ICT diperolehi dari sumber yang dipercayai dan mestilah dinilaikan secara pragmatik. BPM mesti mengambil langkah-langkah yang tertentu	BPM

	untuk mengawal risiko tersebut.	
Dokumen Berkaitan	Sila rujuk kepada topik berikut untuk penyataan dasar yang spesifik: a. Dasar Keselamatan Pembinaan Sistem b. Dasar Keselamatan Sistem c. Dasar Keselamatan Operasi	

09: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Mekanisma Pelaporan Insiden Keselamatan ICT		
Objektif	Memastikan sebarang insiden yang berkaitan dengan sistem ICT dilaporkan dengan kadar segera supaya tindakan boleh diambil secepat mungkin	
090101	**Melaporkan Insiden Keselamatan atau Kerosakan**	
	Semua insiden keselamatan atau kerosakan yang dijumpai/disyaki di dalam sebarang sistem ICT hendaklah dilaporkan kepada ICTSO secepat mungkin. Pengguna dilarang mengambil tindakan sendiri untuk membetulkan keadaan jika terjadinya insiden keselamatan. Pengguna mestilah mengetahui kewujudan prosedur untuk melapor insiden keselamatan. Sila rujuk kepada Surat Pekeliling Am Bil. 4 Tahun 2006: Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT.	Semua
Pengurusan dan Penambahbaikan Insiden Keselamatan ICT		
Objektif	Mewujudkan saluran pelaporan insiden keselamatan ICT yang membolehkan tindakan pemulihan dijalankan segera	
090201	**Tanggungjawab**	
	ICTSO mestilah melaporkan segala insiden keselamatan ICT MOA kepada *Government Computer Emergency Response Team (GCERT).* Rujuk kepada Appendik C: Ringkasan Proses Kerja	ICTSO

	Pelaporan Insiden Keselamatan ICT Agensi.	
090202	**Prosedur**	
	Prosedur rasmi untuk insiden keselamatan ICT mestilah ditubuhkan berdasarkan: a. "Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi"; b. "Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam".	BPM
090203	**Proses Pembelajaran dari Insiden Keselamatan ICT**	
	Satu mekanisma perlu diwujudkan untuk membolehkan jenis, jumlah, kos insiden keselamatan ICT dikaji dan dipantau.	BPM
090204	**Pengumpulan Bukti**	
	Bukti mestilah dikumpul, disimpan dan diserah kepada pihak berkuasa yang berkaitan untuk tindakan tatatertib/undang-undang mengikut kesesuaian. Prosedur dalaman mestilah diwujudkan dan dipatuhi untuk proses pengumpulan dan penyerahan bahan bukti untuk tindakan tatatertib yang dikendalikan oleh MOA.	BPM

10: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Aspek Keselamatan ICT berkaitan dengan Pengurusan Kesinambungan Perkhidmatan *(BCM)*		
Objektif	Untuk bertindak balas ke atas sebarang gangguan berkaitan aktiviti harian dan melindungi proses kritikal dari sebarang kerosakan atau bencana	
100101	**Rangka kerja**	
	Satu rangka kerja bagi Pelan Kesinambungan Perkhidmatan *(BCP)* mestilah diselenggarakan untuk memastikan semua pelan wujud, mengambilkira keperluan keselamatan terhadap proses yang kritikal dan mengenali keutamaan ke atas proses ujian dan penyelenggaraan.	Penyelaras BCP
100102	**Dokumentasi mengenai Pelan Kesinambungan Perkhidmatan**	
	Satu proses membina dan menyelenggara Pelan Kesinambungan Perkhidmatan mestilah diwujudkan. Pelan ini akan memastikan proses yang kritikal boleh beroperasi walaupun terjadinya bencana. Prosedur pemulihan untuk sistem ICT yang kritikal mestilah diwujudkan di dalam Pelan Pemulihan Bencana. Pelan Pemulihan Bencana *(DRP)* perlulah disertakan sekali di dalam Pelan Kesinambungan Perkhidmatan. Sila rujuk Dasar Pemulihan Bencana. Salinan pelan ini mestilah disimpan di lokasi lain untuk mengelakkan bencana yang mungkin terjadi di tempat asal simpanan. Pelan bencana perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;	Penyelaras BCP

	b. Senarai kakitangan MOA dan pembekal berserta nombor yang boleh dihubungi (faksimili, telefon dan emel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani bencana; c. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; d. Syarat-syarat pengaktifan pelan dan individu yang diberi kuasa untuk mengistiharkan bencana dan diberi mandat untuk melaksanakan proses pemulihan; e. Sumber pemprosesan alternatif dan lokasi untuk menggantikan sumber yang telah lumpuh; dan f. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.	
100103	**Menilai Keperluan *BCP***	
	Penilaian risiko dan *business impact analysis (BIA)* mestilah dilaksanakan untuk menentukan keperluan membina *BCP*.	Penyelaras BCP
100104	**Program Latihan dan Kesedaran *BCP***	
	Semua kakitangan mestilah diberitahu tentang *BCP* dan tanggungjawab mereka ke atasnya.	Penyelaras BCP
100105	**Ujian *BCP***	
	BCP mestilah diuji setiap 12 bulan atau bila ada perubahan yang berlaku terhadap aktiviti persekitaran dan fungsi untuk memastikannya efektif. Maklumat yang dikutip semasa proses penilaian mestilah dimasukkan ke dalam *BCP* untuk	Penyelaras BCP

	memantapkan lagi dokumen tersebut.	
100106	**Penyelenggaraan *BCP***	
	BCP mestilah dinilai kembali setiap 12 bulan untuk memastikan ia masih relevan dan efektif digunakan pada ketika itu.	Penyelaras BCP
Dokumen Berkaitan	Dasar Pemulihan Bencana	

11: PEMATUHAN

Pematuhan Ke Atas Dasar Keselamatan, Standard dan Teknikal		
Objektif	Untuk memastikan pematuhan terhadap dasar keselamatan dan standard organisasi	
110101	**Pematuhan Ke Atas Dasar Keselamatan**	
	Semua kakitangan dimestikan untuk membaca, memahami dan mematuhi Dasar Keselamatan ICT MOA dan sebarang undang-undang dan ketetapan yang wujud.	Semua
110102	**Pematuhan Pemeriksaan Teknikal**	
	Sistem ICT mestilah diperiksa selalu untuk mematuhi standard keselamatan yang ada. Sebarang pematuhan teknikal mestilah dijalankan oleh individu yang kompeten dan dibenarkan.	BPM
Pematuhan Ke atas Keperluan Undang-Undang		
Objektif	Untuk menghindarkan pelanggaran ke atas sebarang undang-undang, ketetapan, perjanjian atau keperluan keselamatan	
110201	**Mengenalpasti Undang-Undang yang Perlu Dipatuhi**	
	Semua kakitangan perlu mengikut undang-undang dan ketetapan seperti berikut: **a. Kawalan Keselamatan Secara Umum** i. *Emergency (Essential Power) Act 1964;* ii. *Essential (Key Points) Regulations 1965;*	Semua

	iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982; iv. Arahan Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985; v. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985; vi. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan. **b. Keselamatan Dokumentasi** i. Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control); ii. Akta Rahsia Rasmi 1972; iii. Akta Arkib Negara 2003; iv. Arahan Teknologi Maklumat; v. Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam; vi. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh; vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (Espionage); viii. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan	

	Akta Rahsia Rasmi (Pindaan) 1976; ix. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan x. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999. **c. Keselamatan Fizikal** i. *Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;* ii. *Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;* iii. *State Key Points;* iv. *Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan;* v. *Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/Jabatan;* vi. *Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan* vii. *Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.* **d. Keselamatan Individu** i. Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti;	

	ii. General Circular Memorandum; iii. Instruction On Positive Vetting Procedure; iv. *Surat Pekeliling Am Sulit Bil.1/1966 - Perkara Keselamatan Tentang Persidangan- Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;* v. *Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;* vi. *Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara tabir Buluh dan Tabir besi;* vii. *Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan* viii. *Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.* **e. Keselamatan ICT** i. *Akta Tandatangan Digital 1997;* ii. *Akta Jenayah Komputer 1997;* iii. *Akta Hak Cipta (Pindaan) 1997;* iv. *Akta Multimedia dan Telekomunikasi 1998;* v. *Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;* vi. *Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat &*	

	Komunikasi (ICT); vii. *Pekeliling Am Bil. 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan* viii. *Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi – Agensi Kerajaan;* ix. *Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan;* x. *Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan;* xi. *Surat Arahan Ketua Pengarah MAMPU berkaitan Pengaktifan Fail Log Server;* xii. *Surat Arahan Ketua Setiausaha Negara - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-agensi Kerajaan;* xiii. *Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005;* xiv. *Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;* xv. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002; dan f. Kesemua 11 domain yang terkandung di dalam dasar keselamatan ICT ini.	

Audit Sistem Maklumat		
Objektif	Untuk memaksimumkan keberkesanan dan untuk meminimumkan gangguan kepada / dari proses audit sistem maklumat.	
110301	**Pematuhan Keperluan Audit**	
	Pematuhan kepada keperluan audit perlu bagi minimumkan 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	BPM

APPENDIK

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT MOA

Nama (Huruf Besar) :	
No. Kad Pengenalan :	
Jawatan :	
Bahagian :	

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

Tanda tangan : _____

Tarikh : _____

Pengesahan *ICT Security Officer*

_____

(Nama *ICT Security Officer*) Tarikh: _____

APPENDIK B: MEDIA SANITISATION GUIDELINE

1.1 Overview

Information communication and technology (ICT) systems capture, process, and store information using a wide variety of media. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorised disclosure of information and to ensure its confidentiality.

1.2 Purpose

This document aids in establishing clear guidelines for media disposition and sanitisation. The guidelines will assist MOA in implementing a media sanitisation program with proper and applicable techniques and controls for sanitisation and disposal decisions, considering the security categorization of the associated system's confidentiality.

1.3 Sanitisation

Sanitisation refers to the general process of removing data from storage media prior to its disposal or transfer of control, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

The issue of media disposition is not driven by the media on which the record is stored, but by the information that forms the record that has been placed on the media. In this regard, deciding which method to use to dispose of the media should be done through a risk assessment of the record itself.

Several different methods can be used to sanitise media. Four of the most common are presented in Table 1: Sanitisation Methods. Individuals should assess the media to be disposed of and determine the future plans for the media. Then, using information in the tables below, decide on the appropriate method for sanitisation. The selected method should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

1.4 Sanitisation Methods

Table 1 : Sanitisation Methods

Method	Description
Disposal	Disposal is the act of discarding media with no other sanitisation considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
Clear /Overwrite	One method to sanitise media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitisation method.
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. The difference between degauss and Secure Erase is the former does not permit recoverability of data while the latter does. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitise magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	Destruction is the most extreme form of sanitisation and ensures that the media is drastically altered and can never be reused. There are various methods for media destruction. • **Disintegration**, **Pulverization or Incineration**. These sanitisation methods are designed to completely destroy the media. They are typically carried out at an outsourced metal

Method	Description
	destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • **Shredding**. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), and optical disks (DVD) must be destroyed by pulverizing or crosscut shredding.

The following diagram summarizes the sanitisation method decision process:

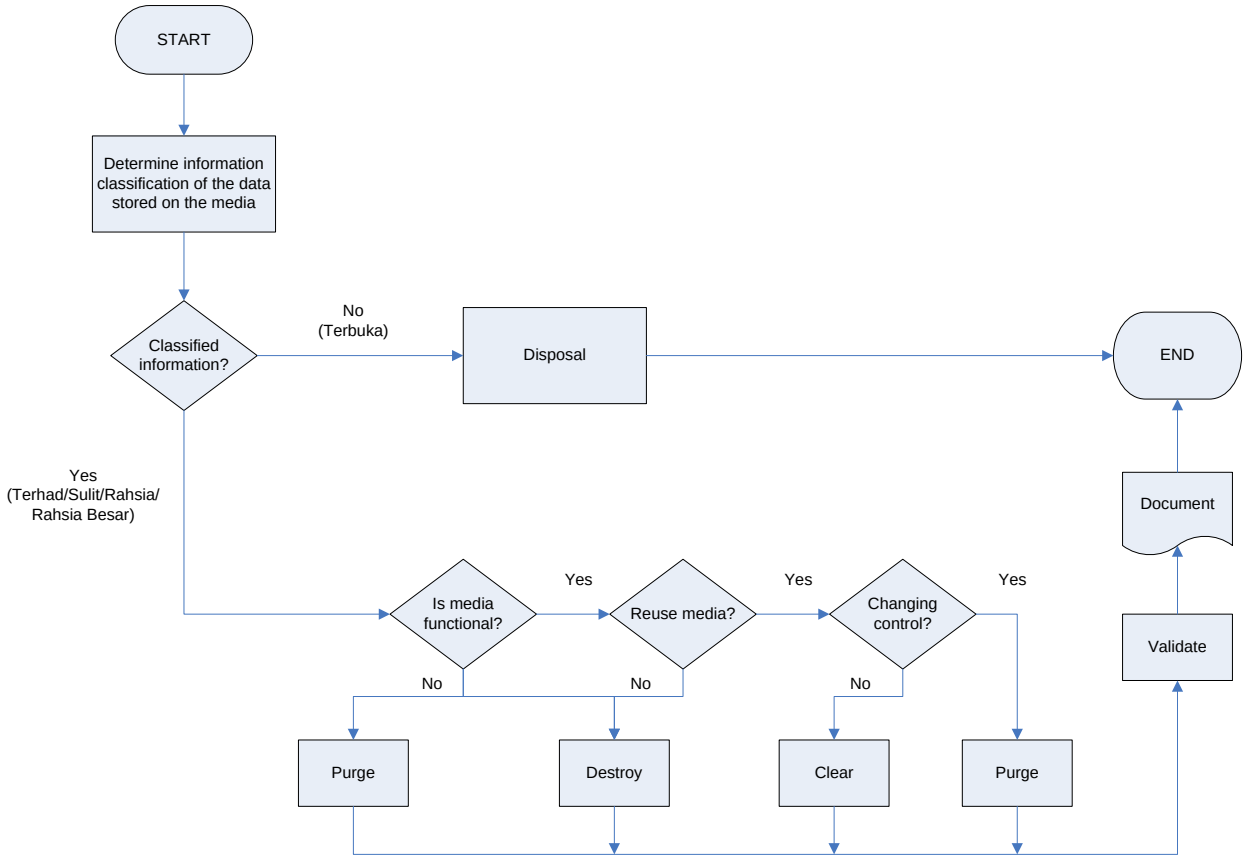


Figure 1: Sanitisation Method Decision Process

1.5 Sanitisation Guidelines

The following table can be used to determine recommended sanitisation of specific media. This recommendation should reflect the security categorization of the media to reduce the impact of harm of unauthorised disclosure of information from the media.

Table 2 : Media Sanitisation Decision Matrix

Media Type	Clear	Purge	Physical Destruction
Hard Copy Storages			
Paper and microforms	See Physical Destruction.	See Physical Destruction.	• Destroy paper using cross cut shredders or pulverize. • Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) cross cut shredders or pulverize.
Hand-Held Devices			
Cell Phones	Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. Contact the manufacturer for proper sanitisation procedure.	Same as Clear.	• Disintegrate. • Pulverize. • Incinerate by burning cell phones in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
Personal Digital Assistant (PDA) Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. Contact the manufacturer for proper sanitisation procedure.	Same as Clear.	• Incinerate PDAss by burning them in a licensed incinerator. • Pulverize.
Networking Devices			
Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings. Contact the manufacturer for proper sanitisation procedure.	Same as Clear.	• Disintegrate. • Pulverize. • Incinerate routers by burning them in a licensed incinerator.
Office Equipment			
Copy/Fax Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings. Contact the manufacturer for proper sanitisation procedure.	Same as Clear.	• Disintegrate. • Pulverize. • Incinerate copy/fax machines by burning them in a licensed incinerator.
Magnetic Disks			
Floppies	Overwrite media by using approved software and validate the overwritten data.	Degauss	• Incinerate floppy disks and diskettes by burning them in a licensed incinerator. • Shred.

Media Type	Clear	Purge	Physical Destruction
ATA Hard Drives	Overwrite media by using approved and validated overwriting technologies/methods / tools.	1. Purge using Secure Erase. 2. Purge hard disk drives by either purging the hard disk drive in an automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with a degaussing wand. 3. Purge media by using approved and validated purge technologies/tools . *Degaussing any current generation hard disk will render the drive <u>permanently</u> unusable.	• Disintegrate. • Pulverize. • Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	Overwrite media by using approved and validated overwriting technologies/methods /tools.	1. Purge using Secure Erase. 2. Purge hard disk drives by either purging the hard disk drive in an automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with a degaussing wand. 3. Purge media by	• Disintegrate. • Pulverize. • Incinerate by burning in a licensed incinerator. .

Media Type	Clear	Purge	Physical Destruction
		using approved and validated purge technologies/tools . *Degaussing any current generation hard disk will render the drive permanently unusable.	
Zip Disks	Overwrite media by using approved and validated overwriting technologies/methods /tools.	Degauss using an approved degausser. * Degaussing any current generation zip disks will render the disk permanently unusable.	• Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. • Shred.
SCSI Drives	Overwrite media by using approved and validated overwriting technologies/methods /tools.	Purge hard disk drives by either purging the hard disk drive in an approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an approved degaussing wand. *Degaussing any current generation hard disk will render the drive permanently unusable.	• Disintegrate. • Pulverize. • Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Magnetic Tapes			

Media Type	Clear	Purge	Physical Destruction
Reel and Casette Format Magnetic Tapes	Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.	Degauss using an approved degausser. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal.	• Incinerate by burning the tapes in a licensed incinerator. • Shred.
Optical Disks			
CDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of recommendations: • Removing the information bearing layers of CD media using a commercial optical disk grinding device. • Incinerate optical disk media using a licensed facility. • Use optical disk media shredders or disintegrator devices.

Media Type	Clear	Purge	Physical Destruction
DVDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of recommendations: • Removing the Information bearing layers of DVD media using a commercial optical disk grinding device. • Incinerate optical disk media using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce DVD into particles.
Memory			
Compact Flash Drives, SD	Overwrite media by using approved and validated overwriting technologies/methods /tools.	See Physical Destruction.	Destroy media in order of recommendations. • Shred. • Disintegrate. • Pulverize. • Incinerate by burning in a licensed incinerator.
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	• Shred. • Disintegrate. • Pulverize.
Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's data sheets.	Same as Clear.	• Shred. • Disintegrate. • Pulverize.

Media Type	Clear	Purge	Physical Destruction
Electronically Erasable PROM (EEPROM)	Overwrite media by using approved and validated overwriting technologies/methods /tools.	Same as Clear.	• Shred. • Disintegrate. • Pulverize. • Incinerate by burning in a licensed incinerator.
Erasable Programmable ROM (EPROM)	Clear media in order of recommendations. 1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations 2. Overwrite media by using approved and validated overwriting technologies/methods / tools.	Same as Clear.	• Shred. • Disintegrate. • Pulverize. • Incinerate by burning in a licensed incinerator.
Flash Cards	Overwrite media by using agency approved and validated overwriting technologies/methods /tools.	Same as Clear.	• Shred. • Disintegrate. • Pulverize.
Flash EPROM (FEPROM)	Perform a full chip purge as per manufacturer’s data sheets.	Purge media in order of recommendations. 1. Overwrite media by using approved and validated overwriting technologies/methods /tools. 2. Perform a full chip purge as per manufacturer’s data sheets.	• Shred. • Disintegrate. • Pulverize. • Incinerate by burning in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use a disintegrator to reduce the card's internal circuit board and components to particles.
RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	• Shred. • Disintegrate. • Pulverize.
ROM	See Physical Destruction.	See Physical Destruction.	• Shred. • Disintegrate. • Pulverize.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using approved and validated overwriting technologies/methods /tools	Same as Clear.	• Shred. • Disintegrate. • Pulverize.
Smart Cards	See Physical Destruction.	See Physical Destruction.	For smart card devices & data storage tokens or cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages), cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder. Smart cards that are not capable of being shredded should instead be destroyed via incineration

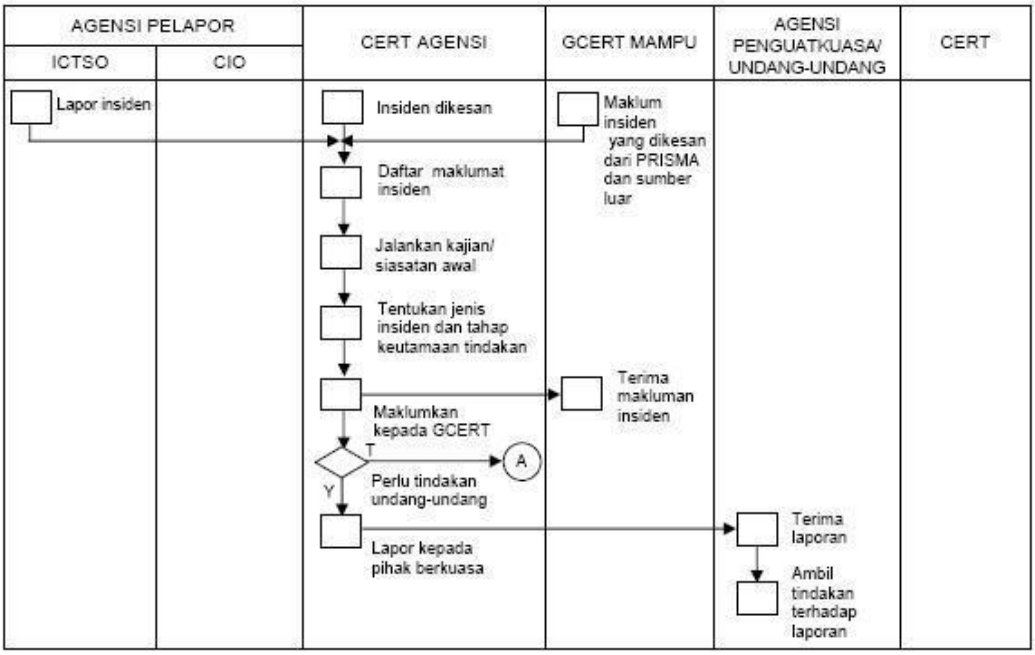
Media Type	Clear	Purge	Physical Destruction
			licensed incinerator or disintegration.

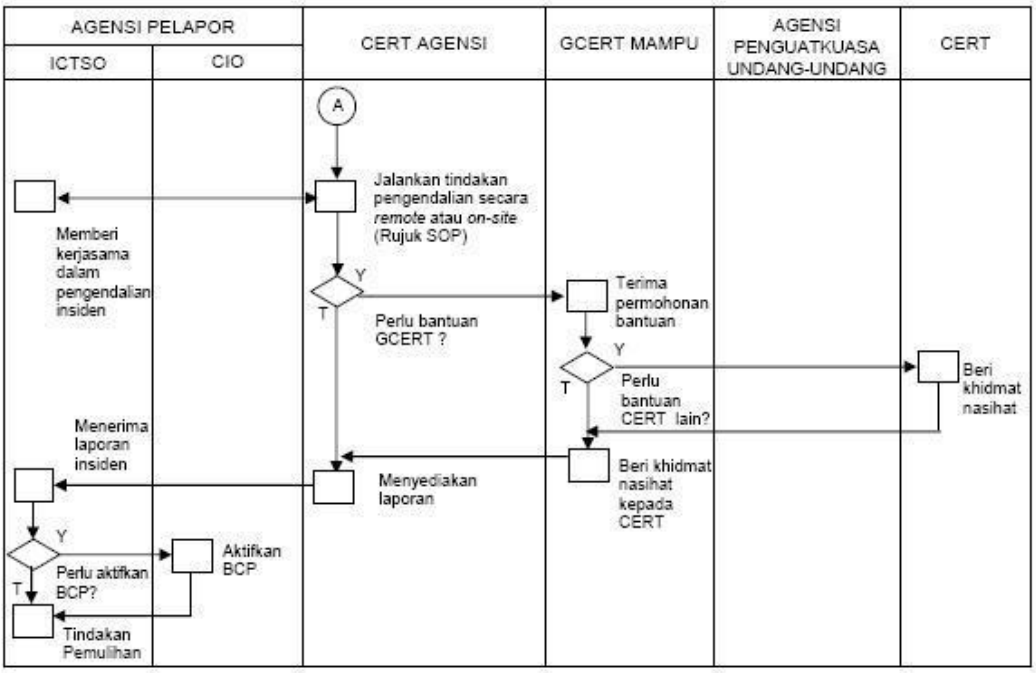
RUJUKAN

"Guidelines for Media Sanitisation : The NIST Handbook (Special Publication 800-88)", United States : National Institute of Standards and Technology, 2006.

APPENDIK C: RINGKASAN PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT AGENSI

Rajah 3 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi





REFERENCES :

Surat Pekeliling Am Bil. 4 Tahun 2006: Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam

APPENDIK D: NON DISCLOSURE AGREEMENT