DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

JABATAN PEGUAM NEGARA (AGC)

JABATAN PERDANA MENTERI

FEBRUARI 2018

Versi 4.0

Diterbitkan oleh:
Jabatan Peguam Negara
Seksyen Teknologi Maklumat, Bahagian Pengurusan
No 45, Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya
Malaysia
Telefon : 03 - 8872 2000
Faks : 03 - 8890 5670
Laman Web : http://www.agc.gov.my

MAKLUMAT DOKUMEN

Tajuk	:	Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT)
Versi	:	4.0
Tarikh Kuat Kuasa	:	15 Februari 2018
Pemilik	:	Seksyen Teknologi Maklumat (STM), Bahagian Pengurusan, Jabatan Peguam Negara

SEJARAH SEMAKAN DAN PINDAAN

TARIKH	VERSI	RINGKASAN SEMAKAN/PINDAAN	KELULUSAN	TARIKH KUATKUASA
10/2008	1.0		2008	
05/2012	2.0	**i. Tajuk baharu : Penilaian Risiko Keselamatan ICT,** **ii. Perkara 020103 Pegawai Keselamatan ICT (ICTSO),** perenggan baru iaitu perenggan (k) menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. **iii. Perkara 020103 Pegawai Keselamatan ICT (ICTSO),** perenggan baru iaitu perenggan (l) Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) AGC. **iv. Perkara 020104 Pengurus IC,** tambahan maklumat Pengurus ICT. **v. Perkara 020104 Pentadbir Sistem ICT,** tambahan meklumat Pentadbir Sistem ICT. **vi. Perkara 020106 Pengguna perenggan (c),** menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat. **vii. Perkara 100101 Pelan Kesinambungan Perkhidmatan,** Pengurus ICT dipinda kepada koordinator PKP. **viii. Perkara 110104 Keperluan Perundangan** pindaan : Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di AGC adalah seperti di Lampiran 3	2012	
09/2013	2.1	i. Seksyen Teknologi Maklumat diganti kepada Pasukan 6 (ICT). ii. Timbalan Pengarah Seksyen Teknologi Maklumat diganti kepada Pegawai Teknologi Maklumat		
12/2015	3.0	**Perubahan Bidang daripada 11 kepada 14 selaras dengan piawaian MS ISO/IEC 27001:2013**	2015	
03/2016	3.1	**Pasukan 6 (ICT) dipinda kepada Seksyen Teknologi Maklumat (STM)**	2016	10 Mac 2016

12/2017	4.0	**i.**	**Pengguguran Bidang 06 Kriptografi.**	2017	15 Februari 2018
		ii.	**Perkara 020105 Pentadbir Sistem ICT/Pentadbir Aplikasi ICT,** penambahan maklumat 'Pentadbir Aplikasi ICT' dan pengguguran perkara (h).		
		iii.	**Perkara 020106 Pasukan Kerja Penilaian Tahap Keselamatan,** penukaran 'Pasukan Kerja Penilaian Tahap Keselamatan' kepada 'Jawatankuasa Keselamatan ICT'.		
		iv.	**Perkara 020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga,** pengemaskinian perkara-perkara yang perlu dilaksanakan oleh Pihak Ketiga sebelum perjanjian dimeterai.		
		v.	**Perkara 020103 Pegawai Keselamatan (ICTSO),** penukaran maklumat Pasukan Tindak balas Insiden Keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA).		
		vi.	**Perkara 050402 Kad Pintar atau Token,** penambahan maklumat 'token'.		
		vii.	**Perkara 070207 Pelupusan Perkakasan**, penukaran peranan 'Pegawai Aset dan Seksyen Teknologi Maklumat AGC' kepada 'Semua'.		
		viii.	**Penukaran Bidang 07 kepada Bidang 06**		
		ix.	**Penukaran Bidang 08 kepada Bidang 07**		
		x.	**Penukaran Bidang 09 kepada Bidang 08**		
		xi.	**Penukaran Bidang 10 kepada Bidang 09**		
		xii.	**Penukaran Bidang 11 kepada Bidang 10**		
		xiii.	**Penukaran Bidang 12 kepada Bidang 11**		
		xiv.	**Penukaran Bidang 13 kepada Bidang 12**		
		xv.	**Penukaran Bidang 14 kepada Bidang 13**		
		xvi.	**Perkara 110202 Pelaporan Insiden,**		

			Penukaran maklumat untuk pelaporan insiden kepada Pasukan Tindakbalas Kecemasan Komputer (CERT),National Cyber Coordination and Command Centre (NC4), Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN)		

ISI KANDUNGAN

PENGENALAN **1**

OBJEKTIF **1**

PERNYATAAN DASAR **1**

SKOP **3**

PRINSIP-PRINSIP **5**

PENILAIAN RISIKO KESELAMATAN ICT **7**

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR **8**

0101 Dasar Keselamatan ICT **8**

010101 Pelaksanaan Dasar 8

010102 Penyebaran Dasar 8

010103 Penyelenggaraan Dasar 9

010104 Pengecualian Dasar 9

BIDANG 02 ORGANISASI KESELAMATAN **9**

0201 Infrastruktur Organisasi Dalaman **9**

020101 Ketua Jabatan 10

020102 Ketua Pegawai Maklumat (CIO) 10

020103 Pegawai Keselamatan ICT (ICTSO) 11

020104 Pengurus ICT 12

020105 Pentadbir Sistem ICT/Aplikasi 12

020106 Jawatankuasa Keselamatan ICT 13

020107 Pengguna Dalaman 14

0202 Pihak Ketiga **15**

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 15

0203 Peralatan Mudah Alih dan Kerja Jarak Jauh **15**

020301 Peralatan Mudah Alih 15

020302 Kerja Jarak Jauh 16

BIDANG 03 KESELAMATAN SUMBER MANUSIA **16**

0301 Keselamatan Sumber Manusia **16**

030101 Sebelum Berkhidmat 16

030102 Dalam Perkhidmatan 17

030103 Bertukar Atau Tamat Perkhidmatan 18

BIDANG 04 PENGURUSAN ASET **18**
0401 Tanggungjawab terhadap aset **18**
040101 Inventori Aset ICT 18
0402 Pengelasan Maklumat **19**
040201 Pengelasan dan Pelabelan Maklumat 19
040202 Pengendalian Maklumat 19
0403 Pengurusan Media **20**
040301 Prosedur Pengendalian Media 20
040302 Media Storan 21
040303 Media Perisian dan Aplikasi 22
040304 Penghantaran dan Pemindahan 22
BIDANG 05 KAWALAN CAPAIAN **23**
0501 Keperluan perniagaan bagi kawalan capaian **23**
050101 Dasar kawalan capaian 23
050102 Capaian kepada rangkaian dan perkhidmatan dalam rangkaian 23
0502 Pengurusan Capaian Pengguna **24**
050201 Akaun Pengguna 24
050202 Hak Capaian 25
050203 Pengurusan Kata Laluan 25
0503 Tanggungjawab Pengguna **26**
050301 Penggunaan maklumat pengesahan diri yang dirahsiakan 26
0504 Kawalan Capaian Sistem Pengoperasian **26**
050401 Capaian Sistem Pengoperasian 26
050402 Kad Pintar atau Token 27
0505 Kawalan Capaian Aplikasi dan Maklumat **28**
050501 Capaian Aplikasi dan Maklumat 28
0506 Kawalan Capaian Rangkaian **28**
050601 Capaian Rangkaian 29
BIDANG 06 KESELAMATAN FIZIKAL DAN PERSEKITARAN **30**
0601 Keselamatan Kawasan **30**
060101 Kawalan Kawasan 30
060102 Kawalan Masuk Fizikal 31

060103 Kawasan Larangan 32
060104 Melindungi daripada ancaman persekitaran dan luaran 32
060105 Bekerja di dalam kawasan terkawal 32
060106 Kawasan penghantaran dan pemunggahan 32
0602 Peralatan **33**
060201 Peralatan ICT 33
060202 Bekalan kuasa dan sokongan lain 35
060203 Keselamatan kabel 35
060204 Penyelenggaraan Perkakasan 36
060205 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat 36
060206 Peralatan di Luar Premis 37
060207 Pelupusan Perkakasan 37
060208 Peralatan tanpa pengawasan 38
060209 *Clear Desk* dan *Clear Screen* 38
0603 Keselamatan Persekitaran **39**
060301 Kawalan Persekitaran 39
060302 Prosedur Kecemasan 40
0604 Keselamatan Dokumen **40**
060401 Dokumen 40
BIDANG 07 KESELAMATAN OPERASI **41**
0701 Prosedur Operasi dan tanggungjawab **41**
070101 Prosedur pengendalian didokumentasikan 41
070102 Pengurusan Perubahan 42
070103 Pengurusan Kapasiti 42
070104 Pengasingan Tugas dan Tanggungjawab 42
0702 Perlindungan dari *malware* **43**
070201 Kawalan terhadap *malware* 43
070202 Perlindungan dari *Mobile Code* 44
0703 *Backup* **44**
070301 *Backup* Maklumat 44
0704 Log dan Pemantauan **45**
070401 Event log 45

070402 Perlindungan maklumat log 46
070403 Log Pentadbir dan Operator 46
070404 Sinkronisasi jam 46
070405 Pengauditan dan Forensik ICT 47
0705 Kawalan terhadap perisian pengoperasian 47
070501 Pemasangan perisian pada sistem pengoperasian 47
0706 Pengurusan Kelemahan Teknikal 48
070601 Pengurusan kelemahan teknikal 48
070602 Halangan pemasangan perisian 48
0707 Audit sistem maklumat 48
070701 Kawalan audit sistem maklumat 48
0708 Kawalan Teknikal Keterdedahan (*Vulnerability*) 49
070801 Kawalan dari Ancaman Teknikal 49
BIDANG 08 KESELAMATAN KOMUNIKASI 49
0801 Pengurusan Keselamatan Rangkaian 49
080101 Kawalan Infrastruktur Rangkaian 49
080102 Keselamatan perkhidmatan rangkaian 50
080103 Pengasingan di dalam rangkaian 51
0802 Pengurusan Pertukaran Maklumat 51
080201 Pertukaran Maklumat 51
080202 Persetujuan dalam pertukaran maklumat 51
080203 Pengurusan Electronic Messaging (E-mel) 51
080204 Kerahsiaan atau *non-disclosure agreements* 53
BIDANG 9 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 53
0901 Keselamatan Dalam Membangunkan Sistem dan Aplikasi 53
090101 Keperluan keselamatan oleh sistem maklumat 53
090102 Memastikan keselamatan perkhidmatan aplikasi kepada oran awam terjamin ... 54
090103 Melindungi transaksi perkhidmatan aplikasi 54
090104 Pengesahan Data *Input* dan *Output* 54
0902 Keselamatan Dalam Proses Pembangunan dan Sokongan 55
090201 Prosedur Kawalan Perubahan 55
090202 Pembangunan Perisian Secara *Outsource* 55

0903 Data ujian **56**

090301 Perlindungan data ujian 56

0904 Keselamatan Fail Sistem **56**

090401 Kawalan Fail Sistem 56

BIDANG 10 HUBUNGAN PEMBEKAL **57**

1001 Keselamatan maklumat di dalam hubungan dengan pembekal **57**

100101 Dasar keselamatan maklumat untuk hubungan pembekal 57

100102 Menangani isu keselamatan dalam skop persetujuan pembekal 57

100103 Rantaian teknologi maklumat dan komunikasi bekalan 57

1002 Pengurusan Penyampaian Pihak Pembekal **58**

100201 Pemantauan dan semakan terhadap perkhidmatan pembekal 58

100202 Pengurusan perubahan kepada perkhidmatan pembekal 58

BIDANG 11 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN **58**

1101 Mekanisme Pelaporan Insiden Keselamatan ICT **58**

110101 Mekanisma Pelaporan 58

1102 Pengurusan Maklumat Insiden Keselamatan ICT **59**

110201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 60

110202 Pelaporan Insiden 60

BIDANG 12 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN **62**

1201 Dasar Kesinambungan Perkhidmatan **62**

120101 Pelan Kesinambungan Perkhidmatan 62

BIDANG 13 PEMATUHAN **64**

1301 Pematuhan dan Keperluan Perundangan **64**

130101 Pematuhan Dasar 64

130102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 64

130103 Pematuhan Keperluan Audit 65

130104 Keperluan Perundangan 65

130105 Pelanggaran Dasar 65

GLOSARI **65**

LAMPIRAN 1 ..... **67**

LAMPIRAN 2 ..... **67**

LAMPIRAN 3 ..... **68**

LAMPIRAN 4 73

PENGENALAN

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

OBJEKTIF

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

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi AGC. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT AGC ialah seperti berikut:

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

PERNYATAAN DASAR

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

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

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

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

a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

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

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

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

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

a) **Perkakasan**

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

b) **Perisian**

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

c) **Perkhidmatan**

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

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

d) **Data atau Maklumat**

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

e) **Manusia**

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

f) **Premis Komputer Dan Komunikasi**

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

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT AGC 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. Kelulusan khas 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 dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah AGC menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

d) **Pengasingan**

Tugas mewujud, memadam, kemas kini, 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 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 AGC hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g) **Pemulihan**

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

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat AGC termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta piawaian. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

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

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

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

BIDANG 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan AGC dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Peguam Negara bertanggungjawab terhadap pembentukan dasar ini dengan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Pengurus ICT dan semua Ketua Bahagian.	Peguam Negara
010102 Penyebaran Dasar	

Dasar ini perlu disebarkan kepada semua pengguna AGC termasuk kakitangan, pembekal, pakar runding dan lain-lain yang berurusan dengan AGC.	Pegawai Keselamatan ICT (ICTSO)
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, piawaian, perundangan dan kepentingan sosial. Piawaian berhubung dengan penyelenggaraan Dasar Keselamatan ICT AGC adalah seperti berikut: a) Mengkaji semula dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis, membuat pembentangan dan mendapatkan kelulusan pindaan daripada Jawatankuasa Pemandu ICT (JPICT) AGC; dan c) Memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pengguna.	Pegawai Keselamatan ICT (ICTSO)
010104 Pengecualian Dasar	
Dasar Keselamatan ICT AGC terpakai kepada semua pengguna ICT AGC dan tiada pengecualian diberikan.	Semua

BIDANG 02 ORGANISASI KESELAMATAN
0201 Infrastruktur Organisasi Dalaman
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT AGC.

020101 Ketua Jabatan	
Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan; b) Mewujudkan dan mengetuai jawatankuasa pengurusan keselamatan ICT AGC; c) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT AGC; d) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT AGC; e) Memastikan semua keperluan keselamatan ICT jabatan (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; f) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT AGC; dan g) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Dasar Keselamatan ICT Kerajaan (Lampiran 1).	Ketua Jabatan
020102 Ketua Pegawai Maklumat (CIO)	
Peranan dan tanggung jawab CIO yang dilantik adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan; b) Membantu Peguam Negara dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c) Menentukan keperluan keselamatan ICT; d) Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan e) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi	CIO

Dasar Keselamatan ICT Kerajaan (Lampiran 1).	
020103 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan; b) Mengurus keseluruhan program-program keselamatan ICT AGC; c) Menguatkuasakan Dasar Keselamatan ICT AGC; d) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT AGC kepada semua pengguna; e) Mewujudkan garis panduan, piawaian dan tatacara selaras dengan keperluan Dasar Keselamatan ICT AGC; f) Menjalankan pengurusan risiko; g) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkannya kepada Ketua Jabatan, CIO dan Pengurus ICT; j) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k) Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT AGC; l) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT AGC;	ICTSO

m) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan n) Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT Kerajaan (Lampiran 1).	
020104 Pengurus ICT	
Ketua Seksyen Teknologi Maklumat merupakan Pengurus ICT AGC. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT AGC; b) Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan AGC; c) Menentukan kawalan akses semua pengguna terhadap aset ICT AGC; d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan; e) Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT AGC dilaksanakan; f) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; dan g) Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT Kerajaan (Lampiran 1).	Pengurus ICT
020105 Pentadbir Sistem ICT/Pentadbir Aplikasi ICT	
Pentadbir Sistem ICT/Pentadbir Aplikasi ICT bagi AGC adalah merujuk kepada : 1. Pegawai Teknologi Maklumat, Unit Sokongan Teknikal (Pentadbir Sistem); 2. Pegawai Teknologi Maklumat, Unit Perancangan dan Pembangunan Sistem (Pentadbir Sistem Aplikasi).	Pentadbir Sistem ICT/ Pentadbir Aplikasi ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT/Pentadbir Aplikasi ICT adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT AGC; b) Menjaga kerahsiaan kata laluan; c) Menjaga kerahsiaan konfigurasi server ICT; d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai semua pengguna ICT Kerajaan yang digantung kerja, berhenti, bersara, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; e) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT AGC; f) Memantau aktiviti capaian harian pengguna; g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; h) Menyimpan dan menganalisis rekod jejak audit; dan i) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Dasar Keselamatan ICT Kerajaan (Lampiran 1).	
020106 Jawatankuasa Keselamatan ICT (JKICT)	
Peranan dan tugas utama Jawatankuasa Keselamatan ICT (JKICT) adalah seperti berikut: a) Menyemak dan mengemas kini semua dasar dan arahan keselamatan yang telah dikeluarkan oleh AGC; b) Menilai kekuatan dan kelemahan amalan kawalan keselamatan fizikal terhadap rangkaian dan sistem ICT AGC; c) Melaksanakan ujian penembusan bagi mengenal pasti	JKICT

kekuatan dan kelemahan keselamatan rangkaian hos AGC; d) Menganalisis dan seterusnya mencadangkan langkah pengukuhan keselamatan rangkaian dan sistem ICT kepada JPICT; e) Menjalinkan hubungan dengan agensi-agensi keselamatan/awam dengan tujuan untuk bertukar-tukar maklumat dan pengalaman; f) Melaksanakan tugas-tugas khas yang diarahkan oleh JPICT.	
020107 Pengguna Dalaman	
Peranan dan tanggungjawab Pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT AGC; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjaga kerahsiaan maklumat kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; d) Menjaga kerahsiaan kata laluan; e) Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; f) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; g) Mengambil bahagian dalam program-program kesedaran mengenai keselamatan ICT (sama ada secara langsung atau tidak langsung); dan h) Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Dasar Keselamatan ICT Kerajaan (Lampiran 1). i) Mengemukakan cadangan bertulis pindaan DKICT. j) Melaporkan insiden keselamatan ICT kepada pihak yang berkenaan.	Pengguna Dalaman

0202 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Akses kepada aset ICT AGC perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dilaksanakan sebelum perjanjian dimeterai: a) Membaca dan memahami Dasar Keselamatan ICT AGC; b) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT AGC (Bagi Pihak Ketiga); c) Melaksanakan Tapisan Keselamatan (Sistem E-Vetting); dan d) Menandatangani Perakuan Akta Rahsia Rasmi 1972;	Pembekal/ Perunding/ Kontraktor
0203 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
020301 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut : a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. b) Peralatan mudah alih hak milik persendirian perlu mendapat	Semua

kebenaran akses capaian rangkaian atau internet daripada pentadbir ICT di AGC sebelum digunakan. c) Sebarang penyalahgunaan peralatan mudah alih hak milik persendirian yang mengakibatkan kebocoran maklumat rasmi AGC boleh dikenakan tindakan tatatertib.	
020302 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut : a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

BIDANG 03 KESELAMATAN SUMBER MANUSIA	
0301 Keselamatan Sumber Manusia	
Objektif: Untuk memastikan semua sumber manusia yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT bagi meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT AGC.	
030101 Sebelum Berkhidmat	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menakrifkan tanggungjawab keselamatan yang berkaitan dalam semua senarai tugas dalam jabatan; c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa	Semua

berdasarkan perjanjian yang telah ditetapkan. d) Membuat semakan latarbelakang bagi semua calon perjawatan selaras dengan undang-undang dan etika bersesuaian dengan keperluan strategik fungsi utama dan klasifikasi maklumat yang akan diakses serta risiko yang berkemungkinan dihadapi.	
030102 Dalam Perkhidmatan	
Seksyen ini bertujuan memastikan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT agensi dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Menjalankan tapisan keselamatan untuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan b) Memastikan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh agensi; c) Memastikan warga AGC yang dilantik mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa; d) Memastikan warga AGC yang menguruskan maklumat terperingkat mematuhi semua peruntukan Akta Rahsia Rasmi 1972; e) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada penjawat awam, dan sekiranya perlu diberi kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; dan f) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan	Semua

sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan AGC.	
030103 Bertukar Atau Tamat Perkhidmatan	
Seksyen ini bertujuan memastikan pertukaran atau tamat perkhidmatan penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan diurus dengan teratur. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan semua aset ICT dikembalikan kepada agensi mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan agensi dan/atau terma perkhidmatan.	Semua

BIDANG 04 PENGURUSAN ASET	
0401 Tanggungjawab terhadap aset	
Objektif: Mengenalpasti dan memberikan tanggungjawab perlindungan yang sesuai kepada semua aset ICT Jabatan Peguam Negara	
040101 Inventori Aset ICT	
Ketua Jabatan bertanggungjawab memastikan semua aset ICT AGC diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) Memastikan semua aset dikenal pasti dan maklumat aset direkodkan dalam borang harta modal dan inventori dan	Pentadbir Sistem dan Semua

sentiasa dikemaskinikan; b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Mengelaskan aset mengikut tahap sensitiviti aset berkenaan; d) Memastikan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; dan e) Setiap pengguna bertanggungjawab terhadap semua aset ICT di bawah tanggungjawabnya.	
0402 Pengelasan Maklumat	
Objektif: Memastikan setiap maklumat menerima tahap perlindungan bersesuaian dengan kepentingannya kepada organisasi	
040201 Pengelasan dan Pelabelan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; atau d) Terhad	Semua
040202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut :	Semua

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 piawaian, piawaian, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. h) Maklumat terperingkat hendaklah disimpan tempat yang berkunci.	
0403 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipenuhi adalah seperti berikut:- a) Melabelkan semua media mengikut tahap sentiviti sesuatu maklumat; b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;	Semua

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 terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut piawaian yang betul dan selamat.	
040302 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 di simpan dalam media storan adalah terjamin dan selamat : a) Menyediakan 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) Media storan sebagai *backup* hendaklah direkodkan pergerakannya. e) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; f) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; Pengguna bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti *thumbdrive* atau *external harddisk* .	Semua

040303 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:- a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan AGC; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Ketua Jabatan; c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-rom, disk atau media berkaitan bagi menggelakkan dari berlakunya kecurian atau cetak rompak; d) Perisian ICT yang tidak berdaftar, berlesen ataupun cetak rompak tidak dibenarkan diguna pakai. Pihak STM AGC berhak membuang (uninstall) perisian tersebut; e) Menyebar perisian cetak rompak melalui kemudahan e-mel AGC adalah di larang; dan f) Aktiviti muat turun (download) atau muat naik (upload) sebarang perisian cetak rompak adalah dilarang. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut piawaian yang ditetapkan.	Semua
040304 Penghantaran dan Pemindahan	
a) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu. b) Media mengandungi maklumat perlu dilindungi daripada sebarang akses, penggunaan atau kerosakan sewaktu di dalam penghantaran atau pemindahan.	Semua

BIDANG 05 KAWALAN CAPAIAN	
0501 Keperluan perniagaan bagi kawalan capaian	
Objektif: Mengawal capaian ke atas maklumat dan pusat pemprosesan maklumat	
050101 Dasar kawalan capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.	Seksyen Teknologi Maklumat, ICTSO dan Semua
050102 Capaian kepada rangkaian dan perkhidmatan dalam rangkaian	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas aset ICT 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.	Seksyen Teknologi Maklumat, ICTSO dan Semua

0502 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas Aset ICT AGC	
050201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan bagi mengenal pasti pengguna dan aktiviti yang dilakukan. Perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh AGC sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan AGC. 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 tidak hadir bertugas tanpa kebenaran melebihi dari tujuh (7) hari; ii. Bertukar ke agensi lain; iii. Bersara; atau	Pentadbir Sistem ICT

iv. Ditamatkan perkhidmatan.	
050202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
050203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta piawaian yang ditetapkan oleh AGC seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Tentukan had masa pengesahan selama sepuluh (10) minit (mengikut kesesuaian sistem) dan selepas had itu,	Pentadbir Sistem ICT

sesi ditamatkan; j) Kata laluan hendaklah ditukar setiap 90 hari; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
0503 Tanggungjawab Pengguna	
Objektif: Meletakkan pengguna dipertanggunjawabkan dalam melindungi maklumat pengesahan pegenalan diri secara rahsia	
050301 Penggunaan maklumat pengesahan diri yang dirahsiakan	
Setiap pengguna adalah diwajibkan mematuhi dan mengamalkan kaedah organisasi di dalam penggunaan maklumat pengesahan pengenalan diri secara rahsia.	Pentadbir Sistem ICT
0504 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian	
050401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal.	Pentadbir Sistem ICT dan ICTSO

Kaedah-kaedah yang digunakan hendaklah AGC menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan piawaian *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Mengehadkan dan mengawal penggunaan program; dan d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
050402 Kad Pintar atau token	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) atau token hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b) Kad pintar atau token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Perkongsian kad pintar atau token untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar atau token yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Seksyen Teknologi Maklumat (STM), Bahagian Pengurusan, AGC.	Semua

0505 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
050501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	dan ICTSO
0506 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	

050601 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian AGC, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisma untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO
050602 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet di AGC hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian AGC; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Peguam Negara atau pegawai yang diberi kuasa;	Pengurus ICT, Pentabir ICT dan Semua

f) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian atau pegawai yang diberi kuasa sebelum dimuat naik ke Internet; h) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh AGC; j) Penggunaan modem/broadband untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

BIDANG 06 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0601 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.	
060101 Kawalan Kawasan	
Keselamatan fizikal adalah bertujuan untuk menghalang,	Semua

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-pelawat; h) Mewujudkan perkhidmatan pengawalan keselamatan; i) Mewujudkan kawasan-kawasan larangan dan terhad;	
060102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Setiap pengguna AGC 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 kaunter pengawal AGC di Blok 4G7; e) Setiap pelawat hendaklah menyerahkan *external storage* dan *mobile phone* di pintu masuk kawasan dan dilarang sama sekali membawa masuk ke bangunan AGC;	Semua

f) Kehilangan pas mestilah dilaporkan dengan segera; g) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT AGC;	
060103 Kawasan Larangan	
Kawasan larangan di Jabatan Peguam Negara adalah bilik Peguam Negara, bilik-bilik Peguam Cara Negara, Peguam Cara Negara II, Unit Penyelidikan Khas, Bilik Fail,Bilik Kebal, Pusat Data di aras 2 4G7, Akses kepada bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : a) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan b) Semua penggunaan peralatan yang melibatkan penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Pentadbir Sistem
060104 Melindungi daripada ancaman persekitaran dan luaran	
Perlindungan secara fizikal daripada bencana alam semulajadi, serangan berniat jahat atau kemalangan perlu diwujudkan dan diimplementasikan di kawasan - kawasan strategik di AGC.	Pentadbir Sistem
060105 Bekerja di dalam kawasan terkawal	
Prosedur bagi bekerja di dalam kawasan terkawal perlu diwujudkan dan diimplementasikan.	Pentadbir Sistem
060106 Kawasan penghantaran dan pemunggahan	
Akses point seperti kawasan penghantaran dan pemunggahan serta kawasan lain di mana individu tanpa kebenaran boleh	Pentadbir Sistem

memasuki premis perlu dikawal dan sekiranya mungkin perlu diasingkan daripada pusat pemprosesan maklumat bagi mengelakkan berlakunya akses tanpa kebenaran.	
0602 Peralatan	
Objektif: Melindungi peralatan ICT AGC dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
060201 Peralatan ICT	
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: 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) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; d) Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; f) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; g) Semua perlatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);	Semua

i) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan yang sesuai; k) Peralatan ICT yang hendak di bawa keluar dari premis AGC, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; l) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; m) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; n) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; o) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; p) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; q) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan 'OFF' apabila meninggalkan pejabat; r) Memastikan plug di cabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti kilat dan sebagainya. s) Penguna adalah dilarang sama sekali menggunakan *thumbdrive* bagi apa jua urusan kecuali telah mendapat kebenaran daripada Ketua Bahagian; t) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	

060202 Bekalan kuasa dan sokongan lain	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS (*Uniterruptible Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kiritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Seksyen Teknologi Maklumat, AGC dan ICTSO
060203 Keselamatan kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan 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 bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Seksyen Teknologi Maklumat, AGC dan ICTSO

060204 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Pegawai Aset dan Seksyen Teknologi Maklumat, AGC
060205 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 atasan dan tertakluk kepada tujuan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua

060206 Peralatan di Luar Premis	
Bagi perkakasan yang dibawa keluar dari premis AGC, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan AGC: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Semua peralatan yang dibawa di luar premis hendaklah direkod dan mendapat kebenaran pegawai atasan. Bagi komputer peribadi, komputer riba dan peralatan lain dalam simpanan STM hendaklah mendapat kebenaran pengurus ICT. Manakala peralatan di bahagian hendaklah mendapat kebenaran Ketua Bahagian masing-masing.	Semua
060207 Pelupusan Perkakasan	
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa dan perlu merujuk kepada Pekeliling Perbendaharaan Bil. 5 tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Jabatan Peguam Negara: a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding (kisar), disguising (menyamar)* atau pembakaran; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Pegawai aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e) Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan	Semua

tersebut; f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori SPPA; g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti *RAM, hard disk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan ICT yang hendak dilupuskan; iii. Memindah keluar dari AGC mana-mana peralatan ICT yang hendak dilupuskan; iv. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer di salin sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
060208 Peralatan tanpa pengawasan	
Pengguna perlu memastikan peralatan tanpa pengawasan secara berterusan mempunyai perlindungan yang bersesuaian.	Semua
060209 ***Clear Desk* dan *Clear Screen***	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.	Semua

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	
0603 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT AGC dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
060301 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 diambil : a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan perkomputeran 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 perkomputeran; e) Semua bahan cecair hendaklah diletakkan di tempat yang	Semua

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.	
060302 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah membaca, memahami dan mematuhi piawaian kecemasan dengan merujuk kepada Garis Panduan Keselamatan AGC; dan b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras;	Semua
0604 Keselamatan Dokumen	
Objektif: Melindungi maklumat AGC dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
060401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut piawaian keselamatan; c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut piawaian Arahan	Semua

Keselamatan; d) Pelupusan dokumen hendaklah mengikut piawaian keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

BIDANG 07 KESELAMATAN OPERASI	
0701 Prosedur Operasi dan tanggungjawab	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
070101 Prosedur pengendalian didokumentasikan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumentasikan, disimpan dan dikawal; b) Setiap prosedur mestilah mengandungi arahan-arahan yang lengkap, teratur dan jelas 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

070102 Pengurusan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan piawaian mestilah mendapat kebenaran daripada pengurus ICT 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.	Semua
070103 Pengurusan 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 dan ICTSO
070104 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi	Pengurus ICT dan ICTSO

mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	
0702 Perlindungan dari *malware*	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh *malware*.	
070201 Kawalan terhadap *malware*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), dan mengikut piawaian penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian tulen yang berdaftar dilindung di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d) Mengemas kini *pattern* anti virus terkini dari semasa ke semasa; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti	Semua

kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; dan h) Mengadakan program dan piawaian jaminan kualiti ke atas semua perisian yang dibangunkan. i) Mengedar amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT Jabatan Peguam Negara.	
070202 Perlindungan dari *Mobile Code*	
Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
0703 *Backup*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
070301 *Backup* Maklumat	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan di simpan dalam lokasi yang selamat. a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat *backup* ke atas semua data dan maklumat mengikut kesesuaian operasi, kekerapan salinan bergantung pada tahap kritikal maklumat;	STM, AGC

c) Menguji sistem *backup* dan piawaian *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Menyimpan sekurang-kurangnya tiga(3) generasi *backup;* dan e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	
0704 Log dan Pemantauan	
Objektif: Merekod *event* dan menghasilkan bukti	
070401 Event log	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan sesuatu acara. Jejak audit hendaklah mengandungi maklumat berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi indentiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian Piawaian untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala.	Pentadbir Sistem ICT

Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya.	
070402 Perlindungan maklumat log	
Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta-arkib Negara. Pengurus 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. Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO. Menyediakan kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan capaian hanya yang dibenarkan.	Pentadbir Sistem ICT
070403 Log Pentadbir dan Operator	
Aktiviti pentadbir dan operator sistem perlu direkodkan dan dilindungi. Semakan secara berkala perlu dilakukan terhadap rekod-rekod log tersebut.	CIO, ICTSO, Pengurus ICT
070404 Sinkronisasi jam	

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam AGC atau domain keselamatan perlu diselaraskan dengan satu sumber AGC yang dipersetujui.	CIO, ICTSO, Pengurus ICT
070405 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara -perkara berikut: a) Sebarang pencerobohan kepada sistem ICT AGC; b) Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery fishing), pencerobohan (intrusion), ancaman (treats) dan kehilangan fizikal (phisical loss); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti-kerajaan; e) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian; f) Aktiviti penyalahgunaan akaun e-mel; dan g) Aktiviti penukaran alamat IP (IP Address) selain daripada yang telah diperuntukkan tanpa kebenaran pentadbir sistem ICT.	ICTSO
0705 Kawalan terhadap perisian pengoperasian	
Objektif: Memastikan integriti sistem pengoperasian	
070501 Pemasangan perisian pada sistem pengoperasian	
Prosedur kawalan pemasangan perisian pada sistem pengoperasian perlu diwujudkan dan diimplementasikan bagi	CIO, ICTSO, Pengurus ICT

mengawal aktiviti pemasangan perisian pada sistem pengoperasian.	
0706 Pengurusan Kelemahan Teknikal	
Objektif: Menghalang eksploitasi terhadap kelemahan teknikal	
070601 Pengurusan kelemahan teknikal	
Maklumat berkaitan kelemahan teknikal bagi sistem maklumat perlu diperolehi di dalam tempoh masa yang terkawal, dengan penilaian terhadap risiko yang dihadapi oleh organisasi terhadap kelemahan teknikal tersebut dinilai dan tindakan pencegahan bersesuaian diambil bagi mengatasi risiko tersebut.	CIO, ICTSO, Pengurus ICT
070602 Halangan pemasangan perisian	
Peraturan berkaitan pemasangan perisian oleh pengguna perlu diwujudkan dan dikuatkuasakan. Pengguna tidak dibenarkan membuat pemasangan sebarang perisian tanpa kebenaran daripada ICTSO.	CIO, ICTSO, Pengurus ICT
0707 Audit sistem maklumat	
Objektif: Meminimumkan impak aktiviti audit terhadap sistem pengoperasian	
070701 Kawalan audit sistem maklumat	
Aktiviti dan keperluan audit melibatkan pengesahan sistem pengoperasian perlu dirancang dengan berhati-hati dan mengambilkira gangguan minimum pada proses perniagaan.	CIO, ICTSO, Pengurus ICT

0708 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesananya.	
070701 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

BIDANG 08 KESELAMATAN KOMUNIKASI	
0801 Pengurusan Keselamatan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
080101 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.	STM, AGC

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan AGC; g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat AGC; i) Memasang *Web Content Filtering* untuk menyekat aktiviti yang dilarang; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan AGC adalah tidak dibenarkan; k) Semua pengguna hanya dibenarkan menggunakan rangkaian AGC sahaja dan penggunaan modem adalah dilarang sama sekali; dan l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
080102 Keselamatan perkhidmatan rangkaian	

080103 Pengasingan di dalam rangkaian	
Kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat perlu diasingkan di dalam rangkaian.	Pentadbir Sistem ICT
0802 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara AGC dan agensi luar terjamin.	
080201 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi seperti berikut: a) Dasar, piawaian dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi.; b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di AGC dengan agensi luar; c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari AGC; dan d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
080202 Persetujuan dalam pertukaran maklumat	
Persetujuan perlu dicapai dalam melaksanakan proses pemindahan secara selamat maklumat perniagaan di antara organisasi dan pihak luaran.	Semua
080203 Pengurusan *Electronic Messaging* (E-mel)	

a) Penggunaan e-mel di AGC hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa. b) Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: c) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh AGC sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; d) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh AGC; e) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan. f) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; g) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; h) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; i) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; j) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; k) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; l) Pengguna hendaklah menentukan tarikh dan masa sistem	Semua

komputer adalah tepat; m) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; n) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan; o) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
080204 Kerahsiaan atau *non-disclosure agreements*	
Keperluan untuk kerahsiaan atau *non-disclosure agreements* selari dengan keperluan organisasi untuk perlindungan terhadap maklumat perlu dikenal pasti, disemak secara berkala dan didokumentasikan.	Semua

BIDANG 09 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
0901 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
090101 Keperluan keselamatan oleh sistem maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti beri a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem *output* untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
090102 Memastikan keselamatan perkhidmatan aplikasi kepada orang awam terjamin	
Perkhidmatan aplikasi yang melalui rangkaian awam perlu dilindungi terhadap sebarang aktiviti tidak sah, percanggahan dengan kontrak dan pendedahan serta pengubahan maklumat tanpa kebenaran.	Pemilik Sistem dan Pentadbir Sistem ICT
090103 Melindungi transaksi perkhidmatan aplikasi	
Perkhidmatan aplikasi yang melalui rangkaian awam perlu dilindungi terhadap sebarang aktiviti tidak sah, percanggahan dengan kontrak dan pendedahan serta pengubahan maklumat tanpa kebenaran.	Pemilik Sistem dan Pentadbir Sistem ICT
090104 Pengesahan Data *Input* dan *Output*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

0902 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
090201 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikutkeperluan sahaja; d) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	STM (AGC), dan Pentadbir Sistem ICT
090202 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik AGC.	Pentadbir Sistem ICT

0903 Data ujian	
Objektif: Memastikan data yang digunakan untuk ujian sistem dilindungi	
090301 Perlindungan data ujian	
Data ujian perlu dipilih dengan sewajarnya, dilindungi dan dikawal dari sebarang capaian tidak sah.	Pentadbir Sistem ICT
0904 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik.	
090401 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut piawaian yang telah ditetapkan; b) Kod atau aturcara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT

BIDANG 10 HUBUNGAN PEMBEKAL	
1001 Keselamatan maklumat di dalam hubungan dengan pembekal	
Objektif: Memastikan aset yang diakses oleh pembekal dilindungi.	
100101 Dasar keselamatan maklumat untuk hubungan pembekal	
Keperluan keselamatan maklumat di dalam mengurangkan risiko berkaitan dengan akses pembekal terhadap aset organisasi perlu diwujudkan dan dilaksanakan dengan persetujuan pihak pembekal dan ianya perlu didokumentasikan.	Seksyen Teknologi Maklumat
100102 Menangani isu keselamatan dalam skop persetujuan pembekal	
Semua keperluan keselamatan maklumat berkaitan perlu diwujudkan dan dipersetujui oleh setiap pembekal untuk akses, proses, penyimpanan, komunikasi, menyediakan komponen infrastruktur IT atau maklumat organisasi.	Seksyen Teknologi Maklumat
100103 Rantaian teknologi maklumat dan komunikasi bekalan	
Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Seksyen Teknologi Maklumat

1002 Pengurusan Penyampaian Pihak Pembekal	
Objektif: Untuk mengekalkan tahap yang dipersetujui keselamatan maklumat dan penyampaian perkhidmatan selaras dengan pembekal perjanjian.	
100201 Pemantauan dan semakan terhadap perkhidmatan pembekal	
Organisasi perlu memantau, membuat semakan dan audit secara berkala terhadap perkhidmatan pembekal.	Semua
100202 Pengurusan perubahan kepada perkhidmatan pembekal	
Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mengekalkan dan meningkatkan dasar keselamatan maklumat sedia ada, prosedur dan kawalan akan di uruskan dengan mengambil kira tahap kritikal maklumat perniagaan, sistem dan proses dan penilaian risiko.	Semua

BIDANG 11 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	
1101 Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden Keselamatan ICT.	
110101 Mekanisma Pelaporan	
Insiden keselamatan ICT bermaksud musibah (adverse event)	Semua

yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CERT AGC 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; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di AGC sepertimana **Lampiran 3**. Piawaian pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
1102 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	

110201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada AGC. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO
110202 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 mekanisma kawalan akses hilang, dicuri atau didedahkan atau disyaki hilang, dicuri atau didedahkan;	Semua

d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini.

Maklumat untuk pelaporan insiden adalah:-

1. AGC Computer Emergency Response Team (AGC CERT)

Alamat	:	Seksyen Teknologi Maklumat, Aras 2, No 45, Persiaran Perdana, Presint 4 Pusat Pentadbiran Kerajaan Persekutuan 62100 Putrajaya
Telefon	:	03-8886 2732/2733 (Waktu Pejabat)
Faks	:	03 - 8890 5670 (Waktu Pejabat)
E-mel	:	cert.agc@agc.gov.my
Portal	:	http://www.agc.gov.my
Waktu Pejabat	:	Isnin - Jumaat 07:30 pagi - 05:30 petang

2. Pasukan Tindakbalas Kecemasan Komputer (CERT)

Alamat	:	Pasukan Tindakbalas Kecemasan Komputer (CERT), National Cyber Coordination and Command Centre (NC4), Agensi Keselamatan Siber Negara (NACSA) Majlis Keselamatan Negara (MKN)
Telefon	:	03-80644829
E-mel	:	cert@nc4.gov.my

3. Malaysian Computer Emergency Response Team (MyCERT)

Alamat	:	CyberSecurity Malaysia Level 7, SAPURA@MINES 7, Jalan Tasik, The Mines Resort City 43300 Seri Kembangan Selangor Darul Ehsan Malaysia
Cyber999 *Hotline*	:	1-300-88-2999 (Waktu Pejabat)
Telefon Bimbit	:	019 - 266 5850 (24x7)
SMS	:	CYBER999 <E-mel><INSIDEN> dan hantar ke 15888
Faks	:	03 - 8945 3442 (Waktu Pejabat)
E-mel	:	cyber999@cybersecurity.my
Web	:	http://www.mycert.org.my
Twitter	:	http://www.twitter.com/mycert
Waktu Pejabat	:	Isnin - Jumaat 09:00 pagi - 06:00 petang

BIDANG 12 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1201 Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
120101 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) 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 AGC. Perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan piawaian kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c) Melaksanakan piawaian-piawaian kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d) Mendokumentasikan proses dan piawaian yang telah dipersetujui; e) Mengadakan program latihan kepada pengguna mengenai piawaian kecemasan; f) Membuat *backup* secara berkala; dan g) Menguji dan mengemas kini pelan sekurang-kurangnya	Koordinator PKP AGC

setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; Senarai personel AGC dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; a) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; b) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan c) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. AGC hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 13 PEMATUHAN	
1301 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT AGC	
130101 Pematuhan Dasar	
Setiap pengguna di AGC hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT AGC dan undang-undang atau peraturan-peraturan lain yang berkaitan yang dikuatkuasakan. Semua aset ICT di AGC termasuk maklumat yang disimpan didalamnya adalah hak milik Kerajaan. Peguam Negara/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT AGC selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber AGC.	Semua
130102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua piawaian keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	ICTSO

130103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
130104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di AGC adalah seperti di Lampiran 4.	Semua
130105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT AGC boleh dikenakan tindakan tatatertib.	Semua

Glosari

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui

	kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan
Downloading	Aktiviti muat-turun sesuatu perisian.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (hoaxes).
STM	Seksyen Teknologi Maklumat (STM), Bahagian Pengurusan, AGC

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT AGC

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Cawangan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

b.p Peguam Negara

Tarikh : .....

LAMPIRAN 2

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT AGC
(BAGI PIHAK KETIGA)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Syarikat : .....

Alamat : .....

.....

.....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....

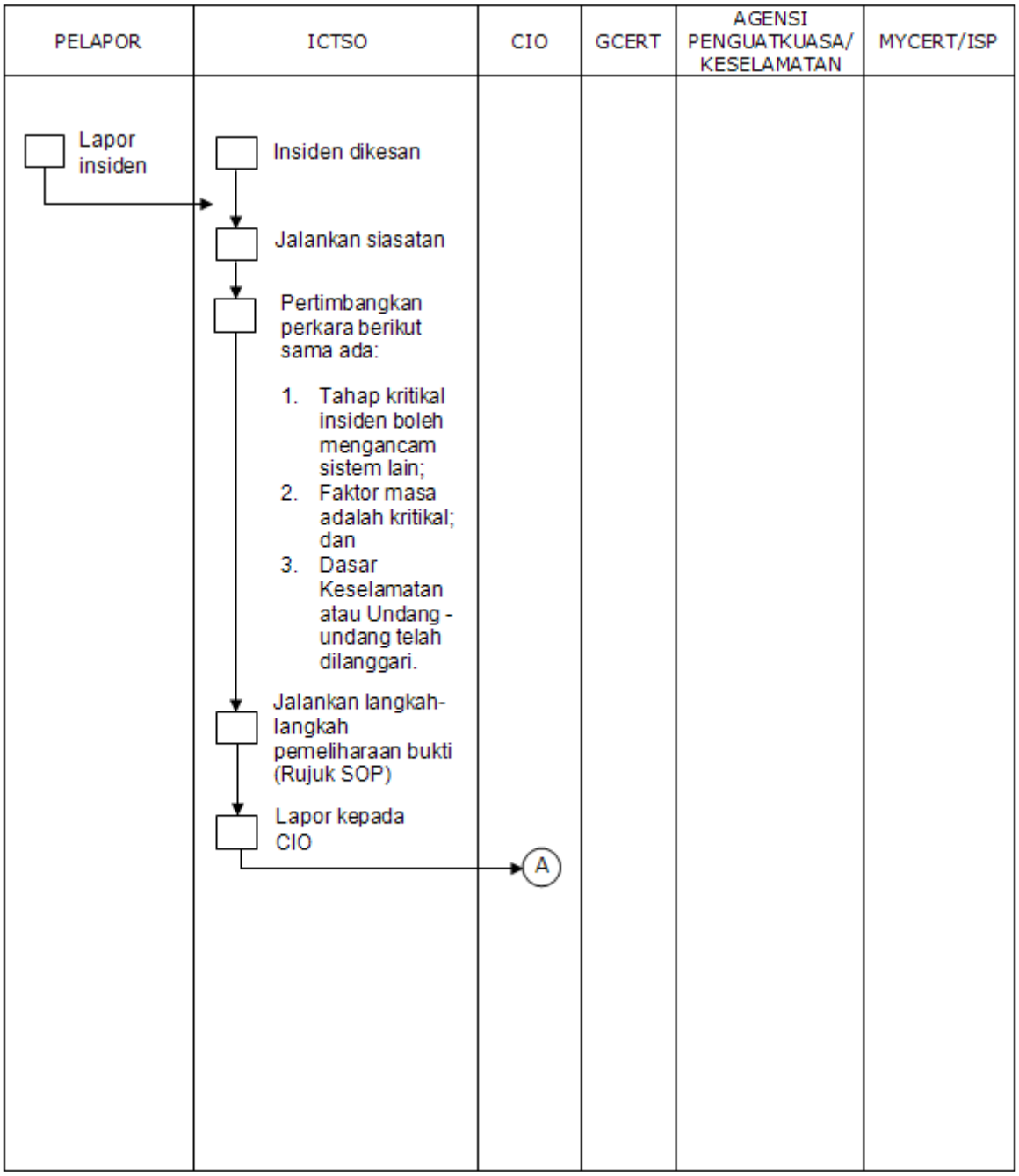
b.p Peguam Negara

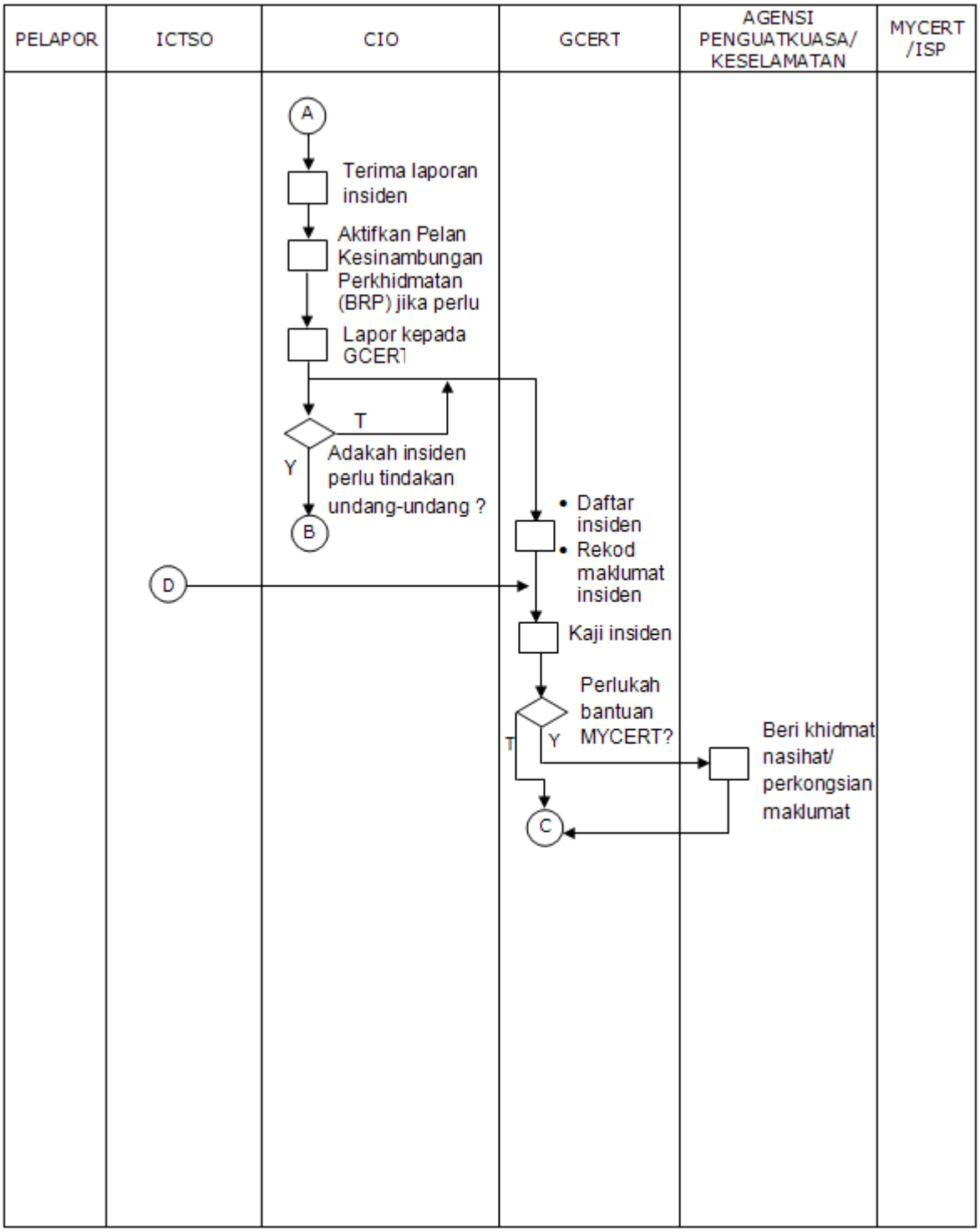
Tarikh : .....

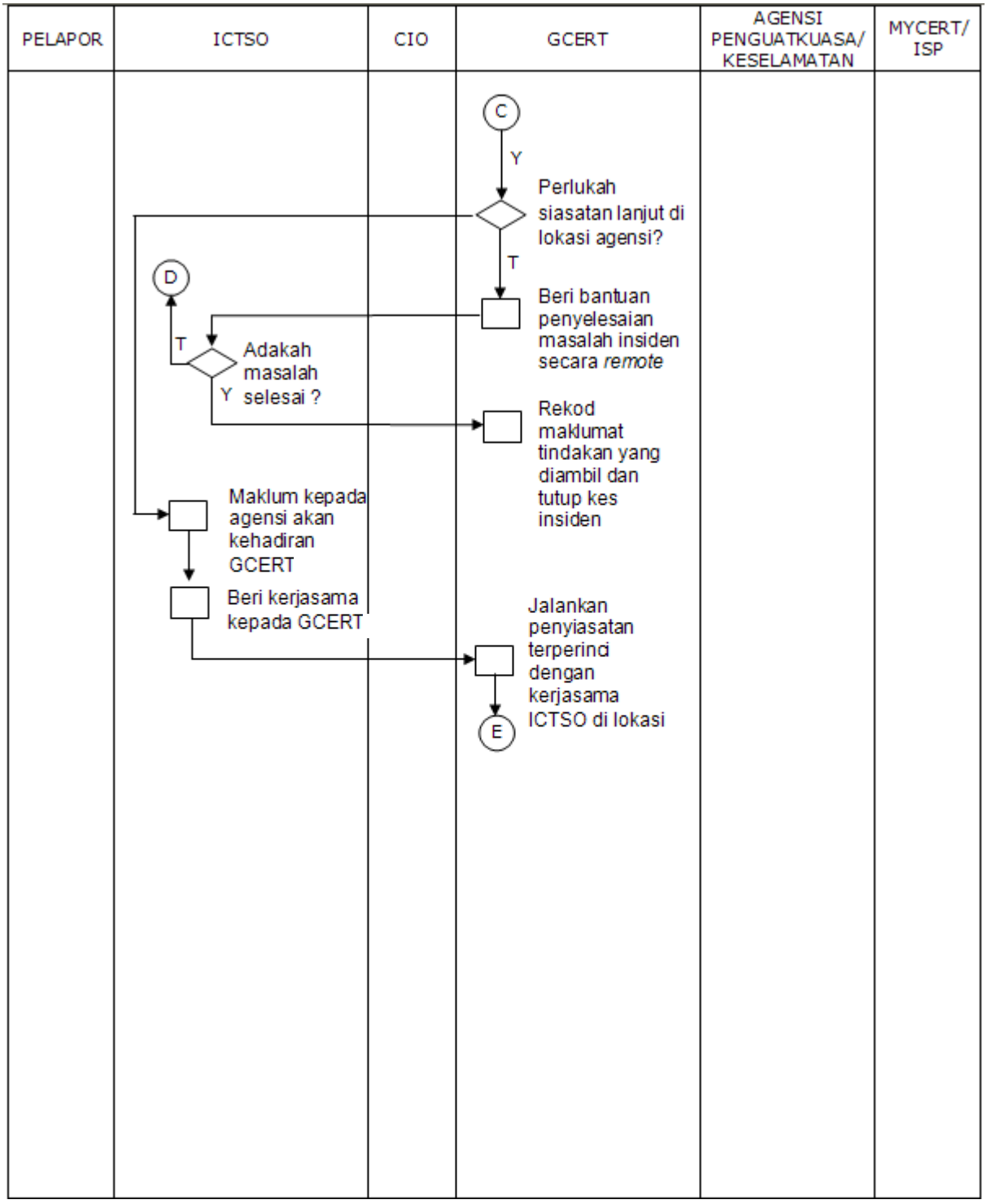
LAMPIRAN 3

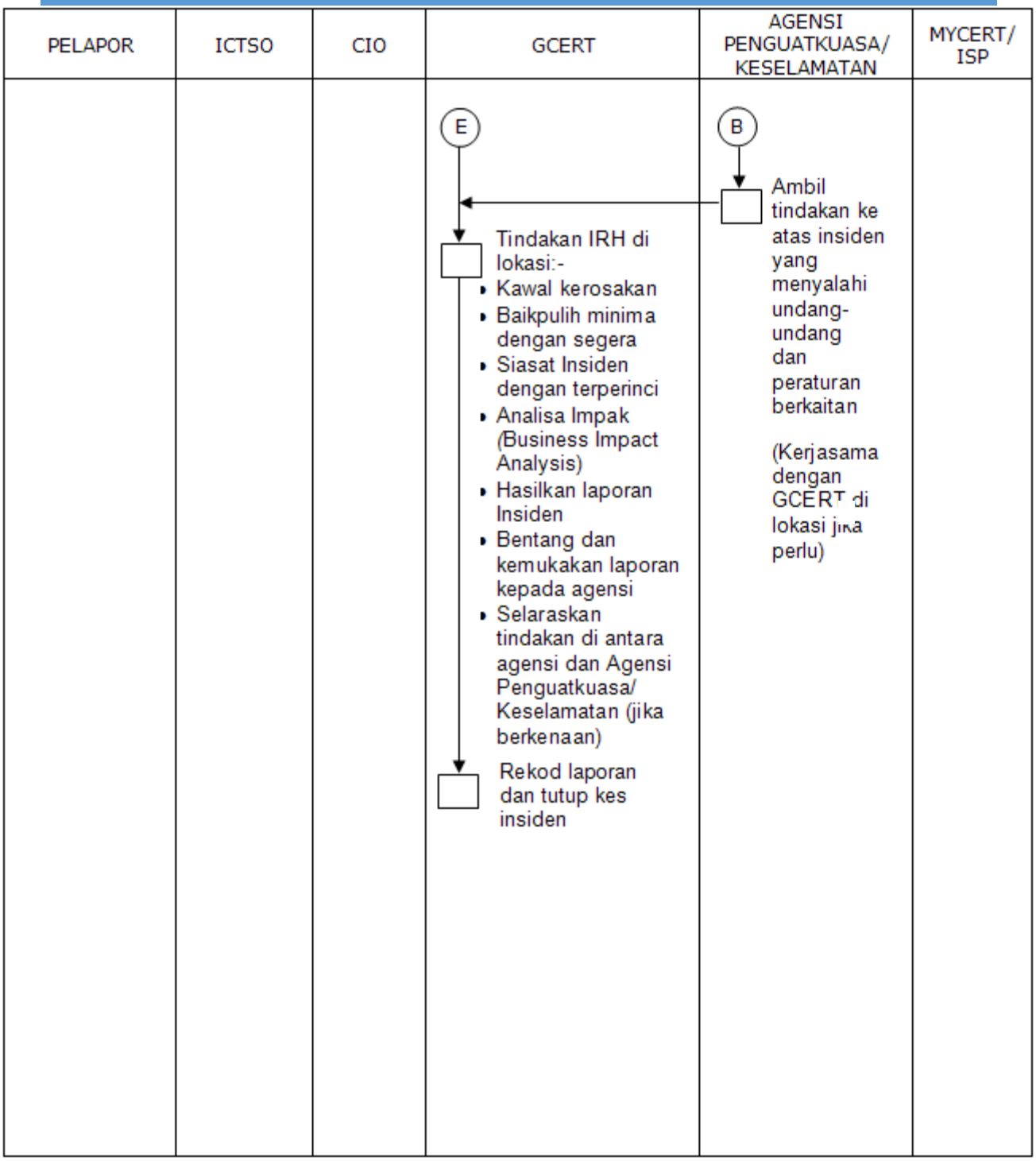
Rajah 1 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT AGC

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselam an ICT MAMPU




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT /ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Y
Adakah insiden perlu tindakan undang-undang ?
B
D
Daftar insiden
Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara remote
D
T
Adakah masalah selesai ?
Y
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
E
B
Ambil tindakan ke atas insiden yang menyalahi undang-undang dan peraturan berkaitan
(Kerjasama dengan GCERT di lokasi jika perlu)
Tindakan IRH di lokasi:-
Kawal kerosakan
Baikpulih minima dengan segera
Siasat Insiden dengan terperinci
Analisa Impak (Business Impact Analysis)
Hasilkan laporan Insiden
Bentang dan kemukakan laporan kepada agensi
Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/ Keselamatan (jika berkenaan)
Rekod laporan dan tutup kes insiden

LAMPIRAN 4

SENARAI PERUNDANGAN DAN PERATURAN

a) Arahan Keselamatan;

b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

d) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - 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) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi- Agensi Kerajaan yang bertarikh 20 Oktober 2006;

i) Surat Arahan Peguam Negara AGC - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

j) Surat Arahan Peguam Negara AGC - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

k) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

n) Akta Tandatangan Digital 1997;

o) Akta Rahsia Rasmi 1972;

p) Akta Jenayah Komputer 1997;

q) Akta Hak Cipta (Pindaan) Tahun 1997;

r) Akta Komunikasi dan Multimedia 1998;

s) Perintah-Perintah Am;

t) Arahan Perbendaharaan;

u) Arahan Teknologi Maklumat 2007;

v) Garis Panduan Keselamatan AGC 2004;

w) Standard Operating Procedure (SOP) ICT AGC;

x) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

y) Surat Arahan Peguam Negara AGC – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.