JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

POLISI KESELAMATAN SIBER
JABATAN PEGUAM NEGARA (AGC)

VERSI 1.0

JABATAN PEGUAM NEGARA (AGC)

JABATAN PERDANA MENTERI

Polisi Keselamatan Siber (PKS)

AGC-ISMS-P1-001

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama: MOHD HOMRI BIN DAUD Penolong Pengarah Kanan Seksyen Teknologi Maklumat Bahagian Pengurusan Jabatan Peguam Negara Jawatan:	Nama: ELIA SUZIANA BINTI MOHAMAD Ketua Penolong Pengarah Kanan Seksyen Teknologi Maklumat Bahagian Pengurusan Jabatan Peguam Negara Jawatan:	Nama: Jawatan: TS. WAHADI BIN MOHAMED Timbalan Pengarah Bahagian Pengurusan Seksyen Teknologi Maklumat Bahagian Pengurusan Jabatan Peguam Negara

JABATAN PEGUAM NEGARA (AGC)

JABATAN PERDANA MENTERI

Polisi Keselamatan Siber

(PKS)

AGC-ISMS-P1-001

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
Nama: .... Jawatan:	Nama: .... Jawatan:	Nama: .... Jawatan:

A. REKOD PINDAAN DOKUMEN

TARIKH	NO. KELUARAN/ PINDAAN	BAB/ MUKA SURAT	KETERANGAN PINDAAN
04 Jun 2024	1.0	Keseluruhan	Versi Awalan

KANDUNGAN

I. RINGKASAN EKSEKUTIF

Secara umumnya, keselamatan siber merujuk kepada bagaimana pengguna Internet menggunakan medium Internet secara positif dan selamat serta melindungi diri mereka daripada ancaman siber.

Amalan keselamatan siber adalah untuk mempertahankan aset siber seperti rangkaian, sistem maklumat dan program atau sistem aplikasi daripada ancaman siber seperti kecurian, kompromi dan/atau serangan. Amalan ini memerlukan pemahaman tentang ancaman maklumat yang berpotensi seperti virus dan kod hasad yang lain. Strategi keselamatan siber termasuklah pengurusan identiti, pengurusan risiko dan pengurusan insiden.

Terdapat 14 bidang kawalan utama Polisi Keselamatan Siber AGC ini dan objektif setiap bidang kawalan adalah seperti yang berikut:

(a) **Bidang 01: Dasar Keselamatan Maklumat**
Bidang ini bertujuan untuk memastikan dasar disemak dan dibangunkan selari dengan hala tuju amalan keselamatan maklumat organisasi.

(b) **Bidang 02: Organisasi Keselamatan Maklumat**
Bidang ini meliputi agihan tanggungjawab bagi tugasan tertentu di samping memastikan organisasi mempunyai rangka kerja yang boleh digunakan bagi mengimplementasi dan menyenggara amalan keselamatan maklumat organisasi.

(c) **Bidang 03: Keselamatan Sumber Manusia**
Tujuan bidang ini adalah untuk memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi keadaan sebelum perkhidmatan, dalam perkhidmatan dan bertukar atau tamat perkhidmatan agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT.

(d) **Bidang 04: Pengurusan Aset**
Bidang ini mengambil perhatian cara organisasi mengenal pasti maklumat dan bentuk perlindungan yang bersesuaian. Tujuan mengenal pasti maklumat adalah bagi menentukan tahap perlindungan yang diperlukan oleh maklumat tersebut.

(e) **Bidang 05: Kawalan Capaian/ Akses**
Bidang ini menerangkan keperluan kawalan akses, pengurusan capaian, kawalan tanggungjawab Pengguna serta kawalan capaian sistem komputer dan sistem aplikasi. Bidang ini juga menerangkan pematuhan penggunaan peralatan mudah alih dan amalan bekerja secara jarak jauh.

(f) **Bidang 06: Kriptografi**
Bidang ini adalah tentang enkripsi data dan pengurusan maklumat sensitif serta memastikan organisasi menggunakan kriptografi dengan betul dan berkesan bagi melindungi kerahsiaan, integriti dan ketersediaan data.

(g) **Bidang 07: Keselamatan Fizikal dan Persekitaran**
Bidang ini menyatakan tentang keselamatan fizikal dan persekitaran organisasi. Tujuan bidang ini adalah untuk mengelakkan akses fizikal yang

tidak dibenarkan, kerosakan kepada premis atau kecurian data sensitif akibat terdedah kepada pindaan, pemusnahan dan akses oleh pihak yang tidak dibenarkan. Di samping itu bidang ini juga menyatakan tentang pengendalian media untuk mengelak daripada berlakunya kehilangan, kerosakan atau kecurian media maklumat seperti perkakasan, perisian atau fail fizikal.

(h) Bidang 08: Keselamatan Operasi
Bidang ini memastikan kemudahan pemprosesan maklumat adalah selamat. Perkara-perkara yang dinyatakan adalah pengoperasian prosedur dan tanggungjawab bagi memastikan operasi yang betul dilaksanakan, memastikan organisasi mempunyai keselamatan yang bersesuaian bagi mengatasi risiko merebaknya malware, keperluan membuat salinan/pendua bagi mengelakkan kehilangan data, memastikan bukti didokumentasikan apabila berlaku kejadian insiden keselamatan siber, melindungi integriti perisian aplikasi, mengelakkan pihak yang tidak dibenarkan mengeksploitasi kelemahan/kerentanan sistem komputer dan meminimakan gangguan ketika pelaksanaan aktiviti audit.

(i) Bidang 09: Keselamatan Komunikasi
Bidang ini memfokuskan kerahsiaan, integriti dan ketersediaan maklumat dalam rangkaian tidak dicerobohi serta memastikan keselamatan data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan.

(j) Bidang 10: Pemerolehan, Pembangunan dan Penyelenggaraan Sistem Aplikasi
Objektif bidang ini adalah untuk memastikan keselamatan maklumat merupakan teras kepada kitar hayat proses di organisasi. Keperluan keselamatan terhadap sistem dalaman organisasi juga melibatkan perkhidmatan yang diberikan menggunakan rangkaian luaran organisasi.

(k) Bidang 11: Hubungan Pembekal
Bidang ini menyatakan keprihatinan tentang perjanjian dengan Pembekal dan Pihak Ketiga terutama perlindungan terhadap aset berharga organsisasi yang diakses oleh Pembekal dan Pihak Ketiga. Di samping itu, tahap keselamatan maklumat dan penyampaian perkhidmatan juga perlu dipersetujui antara organisasi bersama Pembekal dan Pihak Ketiga.

(l) Bidang 12: Pengurusan Pengendalian Insiden Keselamatan Siber
Bidang ini menyatakan tentang proses pengurusan dan pelaporan insiden keselamatan maklumat. Ini melibatkan proses mengenal pasti kakitangan yang patut menjalankan tanggungjawab bagi tindakan tertentu sebagai memastikan pendekatan yang konsisten dan berkesan bagi kitar hayat tindak balas insiden keselamatan maklumat.

(m) Bidang 13: Pengurusan Kesinambungan Perniagaan
Tujuan bidang ini adalah untuk mewujudkan sistem yang berkesan bagi mengurus gangguan kepada bisnes organisasi. Ini melibatkan pembangunan Pelan Kesinambungan Perkhidmatan organisasi yang menggariskan langkah-langkah yang perlu diambil bagi memastikan kesinambungan keselamatan maklumat organisasi.

(n) Bidang 14: Pematuhan
Bidang ini memastikan organisasi mengenal pasti perundangan dan peraturan yang berkaitan keselamatan siber. Ini bagi membantu Pengguna memahami

keperluan kontrak/perjanjian dan undang-undang, mengurangkan risiko ketidakpatuhan dan denda yang terlibat.

(o) **Bidang 15: Threat Intelligence**
Bidang ini menyatakan tentang maklumat yang berkaitan dengan ancaman keselamatan maklumat hendaklah dikumpul dan dianalisis untuk menghasilkan Threat Intelligence.

(p) **Bidang 16: Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud***
Bidang ini menyatakan mengenai penentuan dan pengurusan keselamatan maklumat dalam penggunaan perkhidmatan *cloud*

II. SINGKATAN DAN GLOSARI

Berikut ialah jadual singkatan dan glosari bagi perkataan yang digunakan dalam dokumen ini.

Jadual 1: Singkatan dan Glosari

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
1.	Antivirus	Perisian yang mengimbas virus pada media storan seperti *flash disk* (USB), CDROM untuk sebarang kemungkinan adanya virus.
2.	API (*Application Programming Interface*)	Satu set arahan pengaturcaraan dan standard untuk akses menerusi aplikasi web menggunakan perisian aplikasi web.
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
4.	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus.
5.	*Bandwidth*	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contoh: *video streaming* dan *teleconference*.
6.	*Broadband*	Teknologi yang menyediakan capaian Internet melalui rangkaian luas.
7.	SSM	Seksyen Pengurusan Sumber Manusia
8.	STM	Seksyen Teknologi Maklumat
9.	BYOD (*Bring Your Own Device*)	Peralatan mudah alih persendirian seperti telefon pintar, tablet, komputer riba dan media storan yang digunakan untuk tujuan rasmi.
10.	CSIRT (*Cyber Security Incident Response Team*)	Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu AGC menguruskan pengendalian insiden keselamatan ICT di AGC.
11.	CDO (*Chief Digital Officer*)	Ketua Pegawai Digital, iaitu pegawai yang dilantik untuk menjadi peneraju dalam merancang, melaksana dan memantau program Kerajaan berasaskan ICT bagi memudahkan pelanggan berurusan dengan agensi Kerajaan. Beliau juga merupakan agen transformasi menerusi inovasi, kreativiti dan inisiatif pembaharuan yang berterusan.
12.	CGSO (*Chief Government Security Office*)	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia.
13.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		tempatnya.
14.	*Content Filtering*	Satu teknik yang menyekat atau membenarkan berdasarkan analisis kepada kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian internet dan email.
15.	Data-dalam-simpanan (*Data-at-rest*)	Data yang tidak aktif yang disimpan secara fizikal dalam bentuk digital. Contohnya pangkalan data, gudang data, hamparan, arkib dan sebagainya.
16.	Data-dalam-pergerakan (*Data-in-motion*)	Data transit maklumat digital yang sedang dalam proses pergerakan di dalam atau antara sistem komputer.
17.	Data-dalam-penggunaan (*Data-in-use*)	Data yang sedang diperbaharui, diproses, dihapus, diakses atau dibaca oleh sistem. Jenis data ini tidak disimpan secara pasif, tetapi bergerak aktif melalui infrastruktur IT.
18.	Data Raya	Data yang bersaiz besar (*high-volume*), berubah dengan pantas (*high-velocity*) dan kepelbagaian yang tinggi (*high-variety*).
19.	DDSA	Data *Dictionary* Sektor Awam, iaitu keterangan data yang *standard* untuk diguna pakai oleh agensi-agensi sektor awam.
20.	*Defence-in-depth*	Satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
21.	PKS	Polisi Keselamatan Siber, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT dan ruang siber.
22.	DRP (*Disaster Recovery Plan*)	Pelan Pemulihan Bencana, iaitu dokumentasi pendekatan berstruktur yang menerangkan bagaimana sesebuah organisasi dengan cepatnya memulakan semula kerja setelah berlakunya bencana. DRP merupakan bahagian penting dalam Pelan Pengurusan Kesinambungan Perkhidmatan yang melibatkan aspek-aspek tertentu organisasi yang bergantung kepada infrastruktur ICT.
23.	DTSA (Data Terbuka Sektor Awam)	Data Terbuka Sektor Awam, iaitu inisiatif kerajaan yang menggalakkan perkongsian data, meningkatkan sistem penyampaian perkhidmatan kerajaan dengan lebih mudah, cepat dan telus serta menggalakkan pertumbuhan ekonomi negara. Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan.
24.	E-mel (Mel Elektronik)	Maklumat atau mesej yang dihantar secara elektronik dari satu terminal komputer ke terminal

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		komputer yang lain.
25.	EMS (*Environment Monitoring System*)	Sistem Pemantauan Persekitaran, iaitu sistem yang memantau kualiti persekitaran menggunakan peralatan untuk menilai keadaan dan kecenderungan/trend persekitaran.
26.	Enkripsi (*Encryption*)	Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.
27.	FAT (*Final Acceptance Test*)	Ujian Penerimaan Akhir, iaitu keadaan apabila penyiapan kerja disahkan, dan selalunya setelah ujian-ujian yang perlu telah siap dilaksanakan. Jika terdapat sebarang kecacatan dan kekurangan dikenal pasti, pembetulan perlu dilakukan.
28.	GAMMA (Gallery of Malaysian Government Mobile Application)	Galeri Aplikasi Mudah Alih Kerajaan Malaysia yang menempatkan aplikasi mudah alih agensi Kerajaan bagi kemudahan Pengguna.
29.	GENSET (Generator Set)	Genset atau Janakuasa berfungsi membekal tenaga mekanikal kepada tenaga elektrik.
30.	ICT (Information and Communication Technology)	Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik.
31.	ICT Hijau Kerajaan	Amalan dari segi pengeluaran, penggunaan dan pelupusan komputer, pelayan (server) serta aksesori seperti monitor, tetikus, pencetak dan peralatan rangkaian secara berkesan dan efektif dengan memberi kesan yang minima atau tiada kesan terhadap alam sekitar.
32.	ICTSO (ICT Security Officer)	Pegawai Keselamatan ICT, iaitu pegawai yang dilantik untuk bertanggungjawab terhadap keselamatan siber.
33.	IDS (*Intrusion Detection System*)	Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem diceroboh. Terdapat dua bentuk IDS yang lazim, iaitu pengesanan salah guna dan pengesanan anomali. Dalam pengesanan salah guna, IDS menganalisis maklumat yang dikumpul dan membandingkannya dengan pangkalan data tandatangan serangan yang besar. Secara khusus IDS mencari serangan tertentu yang telah didokumenkan. Seperti sistem pengesan virus, keberkesanan perisian pengesan salah guna ini hanyalah bergantung kepada sebaik mana pangkalan data tandatangan serangan yang ada untuk membandingkan maklumat yang dikumpul.

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
34.	Insiden Keselamatan Siber	Musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar PKS sama ada yang ditetapkan secara tersurat atau tersirat.
35.	Internet	Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.
36.	IP (*Internet Protocol*)	Protokol yang menyalurkan datagram ke saluran yang tertentu dengan harapan ia sampai ke destinasinya.
37.	IPS (*Intrusion Prevention System*)	Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan seperti *malicious code*. Contoh: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
38.	ISMS (*Information Security Management System*)	Sistem Pengurusan Keselamatan Maklumat. ISO/IEC 27001 (ISMS) menyatakan keperluan untuk mewujud, mengoperasi, memantau, mengkaji semula, menyenggara dan memperbaiki Sistem Pengurusan Keselamatan Maklumat organisasi. Pematuhan kepada *standard*/piawaian ISMS ini menunjukkan bahawa sistem pengurusan organisasi perlu memastikan kerahsiaan, integriti dan ketersediaan maklumat.
39.	ISP (*Internet Service Provider*)	Organisasi yang membekalkan pengguna dengan capaian Internet dan khidmat- khidmat yang berkaitan.
40.	Jejak Audit (*Audit Trail*)	Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.
41.	JPICT	Jawatankuasa Pemandu ICT, iaitu jawatankuasa yang memproses, menilai dan mengesyorkan perakuan projek ICT.
42.	JTISA	Jawatankuasa Teknikal ICT Sektor Awam, iaitu jawatankuasa yang menimbang dan meluluskan permohonan kelulusan teknikal daripada agensi sektor awam berdasarkan pelan strategik organisasi dan pelan strategik ICT agensi masing-masing bagi perolehan ICT mengikut had nilai yang telah ditetapkan.
43.	Kawasan Larangan	Kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja.

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
44.	Kawasan Terperingkat	Kawasan yang menempatkan aset ICT berisiko tinggi dan meliputi premis atau sebahagian daripada premis di mana rahsia rasmi disimpan, diuruskan atau di mana kerja terperingkat dijalankan. Akses ke kawasan terperingkat adalah dihadkan dengan kebenaran.
45.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
46.	KPK	Ketua Pegawai Keselamatan, iaitu pegawai yang mengetuai dan bertanggungjawab ke atas semua aspek keselamatan dokumen dan maklumat rasmi, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi selaras dengan peraturan-peraturan yang ditetapkan oleh Kerajaan.
47.	Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.
48.	LAN (*Local Area Network*)	Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat.
49.	Lesen Perisian	Maklumat yang berkaitan pendaftaran, pengesahan lesen bagi membolehkan perisian digunakan secara sah seperti *registration code, serials* dan *CD-keys*.
50.	*Log Out*	Tindakan menarik diri secara rasmi daripada log sistem komputer sebelum berhenti secara muktamad daripada menggunakan sistem.
51.	*Malicious Code*	Sebahagian atau keseluruhan kod atur cara terkompil, skrip, atau jujukan arahan sistem pengendalian atau perisian yang boleh menyebabkan sistem bertindak dengan cara yang tidak diingini oleh Pemilik Sistem dan pengguna. Ia mampu menyebabkan kemudaratan kepada data, pengguna, sumber atau aset sistem komputer yang disasarkan.
52.	Jabatan Digital Negara (JDN)	Jabatan Digital Negara (JDN) ialah sebuah agensi pusat di Jabatan Perdana Menteri yang bertanggungjawab bagi pemodenan pentadbiran dan transformasi sistem penyampaian Perkhidmatan Awam.
53.	Media	Alat atau perantara komunikasi.
54.	Media Sosial	Saluran komunikasi dalam talian yang berasaskan Internet yang membolehkan penggunanya berhubung, bertukar-tukar maklumat, berkongsi idea, bekerjasama dan membina komuniti.

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
55.	Media Storan	Peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *flash disk* (USB), CDROM dan media storan lain.
56.	*Mobile Code*	Kod program yang boleh disebarkan dari komputer ke komputer dan dilaksanakan secara automatik. Contoh: JavaScript, VBScript, applet Java, ActiveX, Flash, Shockwave dan *macro embedded* bagi dokumen Microsoft Office.
57.	Muat turun	Tindakan memindahkan fail atau data daripada sumber tertentu ke komputer pengguna melalui talian rangkaian.
58.	NACSA (National Cyber Security Agency)	Agensi Keselamatan Siber Negara. Ditubuhkan pada Februari 2017 sebagai agensi negara yang menerajui hal ehwal keselamatan siber, dengan objektif memastikan keselamatan dan memperkukuhkan ketahanan Malaysia dalam menghadapi ancaman serangan siber, dengan mengkoordinasi dan mengkonsolidasi pakar-pakar dan sumber negara dalam bidang keselamatan siber.
59.	*Outsource*	Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi tertentu bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui.
60.	Pegawai Data	Pegawai yang dilantik untuk menyelaras dan menyemak set data AGC bagi keperluan penerbitan statistik AGC serta keperluan Data Terbuka untuk dimuat naik ke portal Data Terbuka Sektor Awam.
61.	Pegawai Pengawal	Pegawai yang dilantik oleh Menteri Kewangan atau Menteri Besar atau Ketua Menteri di bawah seksyen 15A Akta Tatacara Kewangan 1957 (Akta 61) bagi setiap tujuan perbelanjaan yang diperuntukkan bagi mana-mana tahun kewangan dalam anggaran, bagi mengawal, tertakluk kepada sebarang arahan yang ditujukan oleh pihak Penguatkuasa Kewangan, perbelanjaan yang dikuatkuasakan di bawah tujuan itu dan termasuk semua tanggungjawab Pegawai Perakaunan.
62.	Pelan Kesinambungan Perkhidmatan	Pelan ini meliputi segala sumber, proses, peranan dan tanggungjawab semua pihak terlibat yang diperlukan sebelum, semasa dan selepas sesuatu gangguan terhadap sistem penyampaian perkhidmatan.
63.	Pelan Pengurusan Krisis Siber Negara dan Prosedur Tindak Balas, Komunikasi dan	Pelan yang dibangunkan berdasarkan kepada rangka kerja pengurusan risiko yang menggariskan strategi bagi mengurangkan kesan serangan siber dan tindak balas yang perlu dilaksanakan oleh

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
	Penyelarasan (NCCMP)	agensi Infrastruktur Maklumat Kritikal Negara (CNII) yang terdiri daripada pelbagai agensi awam dan swasta
64.	Pembekal	Individu, entiti perniagaan atau organisasi yang menyediakan produk atau perkhidmatan kepada Pengguna.
65.	Pemilik Sistem	Pemilik bisnes (*business owner*) bagi sistem yang dibangunkan di AGC yang paling banyak memiliki data dalam sesuatu sistem.
66.	Pengguna	Pegawai dan kakitangan yang berkhidmat secara kontrak atau pegawai khidmat singkat yang menggunakan aset ICT dan siber secara langsung atau tidak langsung.
67.	Pentadbir Sistem ICT	Pentadbir yang melaksanakan dan menyelenggara sistem aplikasi, laman web, media sosial dan aplikasi mudah alih.
68.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT	Pentadbir yang melaksanakan dan menyelenggara Pusat Data, rangkaian ICT dan komunikasi ICT.
69.	Peralatan ICT	Merujuk kepada komponen dalaman perkakasan ICT.
70.	Peralatan Mudah Alih	Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti tablet, *Personal Digital Assistant* (PDA), telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu *Universal Serial Bus* (USB) dan sebagainya.
71.	Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contoh: Linux dan Windows), sistem utiliti (contoh: Disk Cleanup dan Disk Defragmenter) dan perisian aplikasi (contoh: Microsoft Office dan Google Chrome).
72.	Perkakasan ICT	Merujuk kepada peralatan dan perisian ICT.
73.	Penyelaras ICT	Pegawai yang dilantik oleh Pengarah Bahagian untuk memastikan urusan ICT berjalan dengan lancar.
74.	PICT	Pengurus ICT.
75.	Pihak Ketiga	Pakar runding, pihak dan individu yang mempunyai urusan dengan perkhidmatan ICT dan siber serta dilantik untuk melaksanakan tugas di AGC dalam

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		jangka masa yang tertentu.
76.	PII (*Personal Identifiable Information*)	Maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu.
77.	PKI (*Public Key Infrastructure*)	Infrastruktur Kunci Awam, iaitu sistem enkripsi lengkap khusus untuk mencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
78.	PKP	Pengurusan Kesinambungan Perkhidmatan (Business Continuity Management), bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama agensi dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.
79.	Portal DTSA	Portal Data Terbuka Sektor Awam, iaitu data.gov.my yang dibangunkan pada tahun 2014 untuk memudahkan data terbuka kerajaan diakses secara berpusat daripada sumber yang rasmi.
80.	Produk Kriptografi Terpercaya	Produk kriptografi yang dinilai dan diiktiraf oleh Kerajaan bertujuan untuk mengawal dan menjaga keselamatan maklumat, integriti, pengesahan dan tidak boleh disangkal.
81.	PSP (Pelan Strategik Pendigitalan)	Hala tuju strategik pelaksanaan pendigitalan yang akan menjadi panduan bagi memacu agenda Kerajaan Digital yang mampan ke arah membentuk masyarakat digital.
82.	*Restore*	Aktiviti pemulihan atau penyalinan semula data daripada media penduaan.
83.	*Router*	Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. contoh: capaian Internet.
84.	*Screen Saver*	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
85.	*Server*	Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lain yang mempunyai hubungan rangkaian dengannya.
86.	Siber	Ruang maya yang diwujudkan oleh rangkaian komputer sejagat. Ruang tempat berlangsungnya kegiatan pemanfaatan ICT dan internet ini disebut ruang siber.

BIL.	SINGKATAN DAN GLOSARI	KETERANGAN
		Ruang siber (cyberspace) atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari- hari.
87.	Sistem ICT	Merangkumi Sistem Aplikasi, Sistem Pusat Data, Rangkaian dan Komunikasi ICT.
88.	SLA (*Service Level Agreement*)	Perjanjian Tahap Perkhidmatan, iaitu komponen kontrak perkhidmatan antara pembekal perkhidmatan dan pelanggan. SLA menyediakan aspek khusus dan terukur yang berkaitan dengan penawaran perkhidmatan.
89.	SoA (Statement of Applicability)	Dokumen yang memperincikan kawalan- kawalan yang terdapat di Annex A dalam *standard* MS ISO/IEC 27001:2013 *Information Security Management System* (ISMS) bagi menangani risiko keselamatan maklumat bisnes atau maklumat sensitif bisnes.
90.	SPPA	Sistem Pemantauan Pengurusan Aset, iaitu aplikasi yang dibangunkan oleh Kementerian Kewangan untuk tujuan kawalan dan pemantauan aset bagi semua Kementerian dan Jabatan Persekutuan.
91.	*Switch*	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
92.	UAT (*User Acceptance Test*)	Ujian yang dilakukan oleh pengguna/ pelanggan untuk mengesahkan/menerima sistem aplikasi.
93.	UC (*Unified Communication*)	Saluran-saluran komunikasi elektronik selain e-mel yang disepadukan dalam satu rangkaian dan antara muka yang sama.
94.	UPS (*Uninterruptible Power Supply*)	Satu alat yang akan membekalkan kuasa secara automatik kepada peralatan komputer khususnya dan peralatan elektrik umumnya apabila bekalan elektrik utama terputus.
95.	VPN (*Virtual Private Network*)	Teknologi rangkaian atau kaedah yang diguna pakai untuk membuat sambungan rangkaian yang selamat dan menyediakan privasi pada rangkaian peribadi atau awam.
96.	WAN (*Wide Area Network*)	Rangkaian komunikasi yang merangkumi kawasan geografi yang luas di seluruh bandar, negara atau rantau.

III. SENARAI RAJAH

Berikut ialah senarai rajah yang digunakan dalam dokumen ini.

RAJAH	TAJUK
1	Struktur Jawatankuasa ISMS AGC

IV. SENARAI JADUAL

Berikut ialah senarai jadual yang digunakan dalam dokumen ini.

JADUAL	TAJUK
1	Singkatan dan Glosari
2	16 Bidang Kawalan Keselamatan Siber AGC

V. SENARAI PROSEDUR

Berikut ialah senarai prosedur yang digunakan dalam dokumen ini.

PROSEDUR	TAJUK
1	Prosedur Kawalan Perubahan
2	Prosedur Pengurusan Insiden Keselamatan Siber

1.0 PENGENALAN

Polisi Keselamatan Siber (PKS) *Attorney General's Chambers Malaysia* (AGC) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan peralatan ICT dan ruang siber. Peraturan- peraturan ini perlu difahami dan dipatuhi oleh semua Pengguna, Pembekal dan Pihak Ketiga dalam melindungi maklumat di AGC. Dasar ini juga menerangkan kepada semua Pengguna, Pembekal dan Pihak Ketiga mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT dan siber AGC.

2.0 TUJUAN

PKS AGC diwujudkan untuk memastikan pengurusan tadbir urus keselamatan siber bagi semua inisiatif digital AGC dipatuhi bagi meredakan kebimbangan mengenai masalah keselamatan maklumat.

3.0 OBJEKTIF

Objektif utama PKS AGC ialah seperti berikut:

(i) Memastikan kelancaran operasi pendigitalan AGC dan meminimumkan kerosakan atau kemusnahan disebabkan insiden keselamatan siber;

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

(iii) Mencegah salah guna atau kecurian aset ICT dan siber Kerajaan;

(iv) Meminimumkan kos penyelenggaraan aset ICT akibat ancaman, godaman dan penyalahgunaan;

(v) Memperkemaskan pengurusan keselamatan siber AGC; dan

(vi) Menghindari tindakan penggodaman ruang siber yang dituju kepada sistem ICT atau laman web rasmi AGC.

4.0 TADBIR URUS

Secara umumnya, tadbir urus yang baik merupakan satu bentuk mekanisme penyediaan perkhidmatan yang baik untuk masyarakat.

PKS AGC merangkumi:

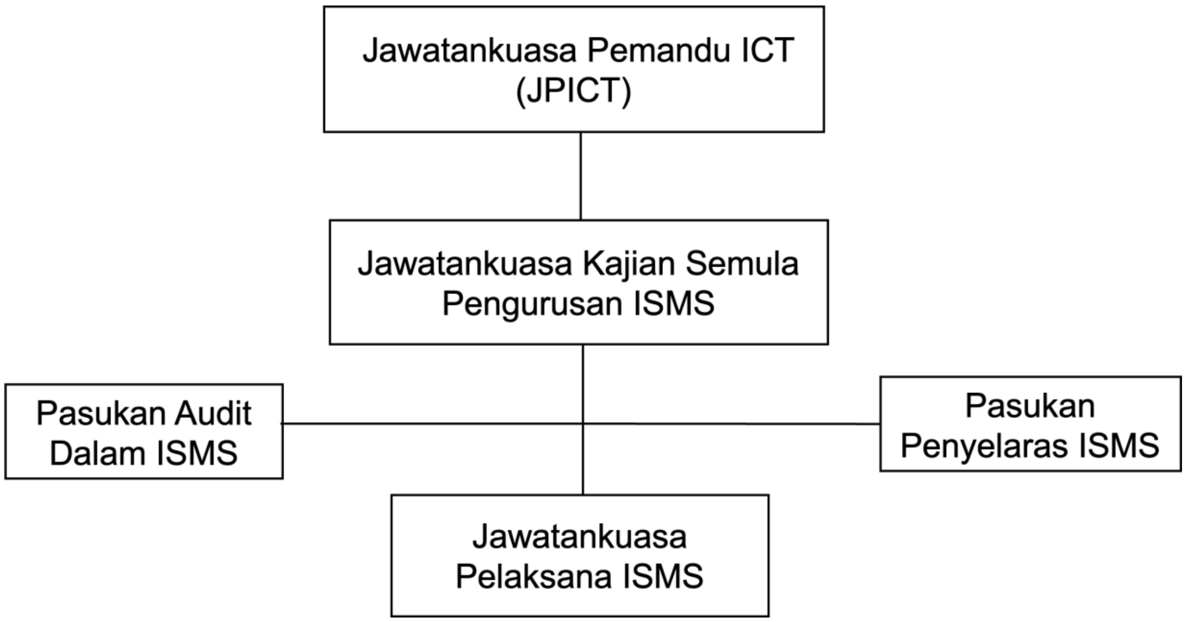
(a) Semua Bahagian AGC.

Tadbir urus dilaksanakan melalui jawatankuasa-jawatankuasa yang ditubuhkan dan peraturan-peraturan yang sedang berkuat kuasa bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS AGC. Antara jawatankuasa tersebut adalah seperti berikut:

(i) Jawatankuasa ISMS AGC; dan
(ii) Jawatankuasa Pemandu ICT (JPICT) AGC.

4.1 JAWATANKUASA ISO/IEC 27001:2013 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AGC.

PKS AGC dibangunkan selaras dengan keperluan ISO/IEC 27001:2022 ISMS yang merupakan amalan terbaik ISO/ IEC 27000 dan standard antarabangsa dalam menetapkan keperluan secara berterusan sistem pengurusan keselamatan maklumat mengikut konteks organisasi. Struktur Jawatankuasa ISMS AGC adalah seperti Rajah 2: Struktur Jawatankuasa ISMS AGC.



Rajah 1: Struktur Jawatankuasa ISMS AGC

Keahlian Jawatankuasa ISMS AGC adalah seperti yang berikut:

Bil.	Peranan	Tanggungjawab
1.	Jawatankuasa Pemandu ICT (JPICT)	a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT AGC; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT AGC;
2.	Jawatankuasa Kajian Semula Pengurusan ISMS	a) Memantau dan menyemak pelaksanaan pensijilan ISMS; b) Menetapkan struktur organisasi ISMS; c) Memantau pelaksanaan pensijilan ISMS AGC; d) Memantau status kemajuan ISMS; e) Meluluskan Polisi Keselamatan Siber (PKS) AGC; f) Meluluskan Skop ISMS; g) Meluluskan Tadbir Urus ISMS; h) Menetap kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko; i) Melaksanakan Mesyuarat Kajian Semula Pengurusan (MKSP) AGC sekurang-kurangnya satu kali (1) setahun; j) Mengesahkan status tindakan daripada kajian semula pengurusan terdahulu; k) Mengesahkan perubahan pada isu luaran dan dalaman yang berkaitan dengan ISMS;dan l) Memantau prestasi keselamatan maklumat termasuk: i) Ketakakuran dan tindakan pembetulan ii) Hasil pemantauan dan pengukuran iii) Hasil audit; iv) Pencapaian objektif keselamatan maklumat; v) Memantau maklum balas daripada pihak berkepentingan; m) Merancang peluang untuk penambahbaikan berterusan.
3.	Jawatankuasa Pelaksana ISMS	a) Melaksana ISMS dengan:

Bil.	Peranan	Tanggungjawab
		i) Menghadiri kursus kesedaran standard ISO/IEC 27001:2022; ii) Melaksanakan prosedur dan kawalan dalam ISO/IEC 27001:2022; dan iii) Melaksanakan tindakan pembetulan / penambahbaikan dan pelan penguraian risiko. iv) Melaksana Mesyuarat Jawatankuasa Pelaksana ISMS AGC sekurang-kurangnya satu kali (1) setahun. b) Menguruskan dokumen dan rekod pelaksanaan ISMS; c) Melantik pasukan audit dalam dan ketua audit dalam ISMS; d) Menyedia kaedah pengukuran keberkesanan kawalan ISMS; e) Mengukur keberkesanan kawalan ISMS; f) Memantau pelaksanaan tindakan pembetulan dan penambahbaikan; g) Memantau dan menyemak semula ISMS; h) Merancang latihan kesedaran standard ISMS; i) Mengenalpasti kompetensi pegawai pelaksana; dan a) Memastikan rekod-rekod latihan diselenggara dengan baik.
4.	Pasukan Penyelaras ISMS	a) Sebagai koordinator dalam menyemak dan mengemaskini prosedur-prosedur berkaitan ISMS; b) Mengawal selia dan menyelaras dokumentasi ISMS; c) Memastikan rekod-rekod pelaksanaan ISMS diselenggara dengan baik; d) Memastikan pasukan pelaksana ISMS merujuk prosedur dan borang yang terkini; e) Melaksanakan kerja-kerja keurusetiaan mesyuarat / bengkel / latihan; dan f) Menguruskan pelaksanaan audit dalam dan audit luar.
5.	Pasukan Audit Dalaman ISMS	a) Menyediakan jadual audit tahunan, jadual pelaksanaan audit dan senarai semak audit;dan

Bil.	Peranan	Tanggungjawab
		b) Melaksana Audit Dalam ISMS AGC berdasarkan kawalan yang diperlukan dalam ISO/IEC 27001:2022; c) Menyediakan Laporan Audit Dalam ISMS; d) Membentang penemuan Audit Dalam ISMS; e) Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan (jika perlu); dan f) Mengemukakan Laporan Audit Susulan (jika perlu).

5.0 PRINSIP-PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada PKS AGC dan perlu dipatuhi mengikut kesesuaian maklumat yang dikendalikan adalah seperti berikut:

a) Akses atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT dan ruang siber 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 dan dibenarkan akses maklumat tersebut.

Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.

b) Hak Akses Minimum

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

c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICTdan ruang siber. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk membolehkan pertanggungjawaban ini dilaksanakan, sistem komputer hendaklah mampu menyokong kemudahan mengesan dan mengesahkan penggunaan sistem komputer.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

(i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(ii) Memeriksa data dan maklumat serta menentukan ianya tepat dan lengkap dari semasa ke semasa;

(iii) Menentukan data dan maklumat sedia untuk digunakan;

(iv) Menjaga kerahsiaan kata laluan;

(v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

(vii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT dan ruang siber daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan sistem dan operasi;

e) Pengauditan

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

f) Pematuhan

PKS AGC hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber;

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 (DRP) dan/atau Pengurusan 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.

6.0 SKOP PKS AGC

Skop PKS AGC merangkumi perkara berikut:

a) Aset ICT dan Siber;

b) Manusia;

c) Proses; dan

d) Teknologi

6.1 ASET ICT DAN SIBER

Ruang siber (cyberspace) atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai kegiatan sehari-hari.

PKS AGC menetapkan keperluan-keperluan asas berikut:

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

b) Data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan integriti dan kesahihan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan ruang siber ini terpelihara keselamatannya sepanjang masa, PKS AGC ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan sebagai sandaran. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan serta prosedur 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, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian yang disimpan dalam sistem komputer. Contoh: perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat 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 kawalan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain- lain.

d) Data dan Maklumat

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

e) Premis Komputer dan Komunikasi

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

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran data dan maklumat atau kelemahan perlindungan dianggap sebagai perlanggaran langkah-langkah keselamatan siber.

6.2 MANUSIA

Pengguna, Pembekal dan Pihak Ketiga hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan hendaklah dibangunkan bagi semua Pengguna AGC.

a) Kompetensi Pengguna

i. Kompetensi pengguna termasuk:

- Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber; dan
- Kemahiran menggunakan alat-alat/tool menjaga keselamatan siber dengan latihan yang mencukupi untuk pelaksanaan tugas rasmi harian.

ii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

iii. Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan selaras dengan arahan/pekeliling semasa adalah dipatuhi.

b) Kompetensi Pelaksana

i. Pengguna yang menguruskan aset ICT dan ruang siber hendaklah memenuhi keperluan kecekapan minimum mengikut tugas mereka.

ii. Pegawai Keselamatan ICT/ICTSO hendaklah memenuhi syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber;
- Memenuhi keperluan pembelajaran berterusan;
- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber; dan
- Menjalani dan memperolehi kelulusan tapisan keselamatan daripada agensi yang diberi kuasa.

iii. Pegawai Keselamatan ICT/ICTSO yang dilantik hendaklah memenuhi keperluan kompetensi di atas. ICTSO bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan siber di AGC.

c) Peranan

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

ii. Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan (NDA) seperti Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

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

iv. Pegawai Aset yang menguruskan aset ICT hendaklah memastikan semua aset ICT AGC dikembalikan sekiranya berlaku perubahan peranan.

v. Pengguna yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset AGC yang berkaitan seperti tersenarai dalam senarai aset pada Nota Serah Tugas.

vi. Pengguna yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset AGC dengan diselia oleh Pegawai Aset yang dipertanggungjawabkan oleh AGC.

6.3 PROSES

Pengguna hendaklah memastikan keselamatan siber dengan melaksanakan perkara-perkara berikut:

a) Konfigurasi Asas

i. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.

ii. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan Prosedur Kawalan Perubahan.

b) Kawalan Perubahan Konfigurasi

i. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

ii. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.

iii. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

c) Sandaran

i. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan sekiranya berlaku sebarang bencana.

ii. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

d) Kitaran Pengurusan Aset

i. Pindah

- Pemindahan hak milik aset berlaku dalam keadaan berikut:
  - Pengguna meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
  - Aset yang dikongsi untuk kegunaan sementara;
  - Pemberian aset kepada agensi lain; dan
  - Aset dikembalikan setelah tamat tempoh sewaan.

- Data dalam peranti tersebut hendaklah diuruskan mengikut Prosedur Pelupusan.

ii. Pelupusan

- Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.
- Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara [Akta 629] dan Peraturan- peraturan Arkib Negara yang sedang berkuatkuasa.
- Pelupusan boleh dilaksanakan dalam bentuk/ kaedah pemusnahan fizikal dan/ atau sanitasi data.
- Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

iii. Kitaran Hayat

- Kitaran hayat data hendaklah diuruskan mengikut Akta Arkib Negara [Akta

629] dan Peraturan-peraturan Arkib Negara yang sedang berkuatkuasa.

- Rekod kewangan hendaklah disimpan selama 7 tahun dan rekod umum selama 5 tahun.

6.4 TEKNOLOGI

Teknologi untuk melindungi data dan maklumat hendaklah dikenal pasti di semua peringkat pemprosesan data dan maklumat di setiap elemen pengkomputeran seperti berikut:

a) Peringkat Pemprosesan Data

i. Data-dalam-simpanan

- AGC hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.
- Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

ii. Data-dalam-pergerakan

AGC hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

iii. Data-dalam-penggunaan

- AGC hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.
- Teknologi yang bersesuaian boleh digunakan oleh AGC untuk memastikan asal data dan data transaksi tanpa-sangkal.

iv. Perlindungan Ketirisan/Kebocoran Data

- Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.
- Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

b) Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan Penilaian Risiko dan Pelan Pengurusan Risiko, AGC hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*counter measure dan control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh CGSO atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di AGC hendaklah mempunyai pengurusan keselamatan maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

i. Peranti Pengkomputeran Peribadi

- Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, *desktop*, telefon pintar, tablet, dan peranti storan.
- Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada AGC. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada Pelan Penguraian Risiko.

ii. Peranti Rangkaian

- Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch, router, firewall*, peranti VPN dan kabel.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

iii. Perisian Aplikasi

- Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

iv. Pelayan

- Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam- penggunaan, data-dalam-pergerakan, data- dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

v. Persekitaran Fizikal

- Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
- Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip defence-in-depth.
- Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diambil kira dalam pengurusan keselamatan maklumat.

7.0 PENILAIAN RISIKO KESELAMATAN SIBER

AGC hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT dan ruang siber supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT dan ruang siber. AGC hendaklah melaksanakan penilaian risiko keselamatan siber secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan siber. Seterusnya mengambil tindakan susulan dan/ atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan siber berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan siber hendaklah dilaksanakan ke atas sistem maklumat AGC termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik penyelenggaraan, kemudahan utiliti dan sistem-sistem sokongan lain. AGC bertanggungjawab melaksanakan dan menguruskan risiko keselamatan selaras dengan keperluan Surat PekelilingArahan/Garis Panduan Penilaian Risiko Keselamatan Maklumat yang sedang berkuatkuasa.

AGC hendaklah 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 atasan;
c) mengelak dan/atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d) memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

8.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di AGC hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain. Pelan ini hendaklah mengenal pasti perlindungan data- dalam-penggunaan, data-dalam pergerakan, data dalam-simpanan dan menghalang ketirisan data dan maklumat.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan surat pekeliling/ arahan terkini untuk menangani isu-isu operasi sesebuah projek.

Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan siber bagi setiap kategori elemen di bawah:

a) Peranti Pengkomputeran Peribadi

i. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada STM, AGC. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

b) Peranti Rangkaian

i. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti switch, router, firewall, peranti VPN dan kabel.

ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data dan maklumat hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

c) Aplikasi

i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.

ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam- pergerakan, data-dalam-simpanan dan menghalang ketirisan data dan maklumat hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

d) Pelayan

i. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam- pergerakan, data-dalam-simpanan dan menghalang ketirisan data dan maklumat hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

e) Persekitaran Fizikal

i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

ii. AGC hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip defence-in-depth.

iv. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam- pergerakan, data-dalam-simpanan dan menghalang ketirisan data dan maklumat hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

9.0 PERNYATAAN POLISI KESELAMATAN SIBER AGC

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

Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem komputer berjalan secara berterusan tanpa gangguan. Keselamatan siber berkait rapat dengan perlindungan aset ICT,manusia dan persekitaran bekerja. Lima (5) komponen asas keselamatan siber adalah seperti berikut:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;

b) Menjamin setiap maklumat adalah tepat dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna;

d) Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat daripada sumber yang sah; dan

e) Menghindari ruang siber dari menimbulkan berbagai ancaman dan potensi ancaman serta gangguan mulai dari skala kecil hingga skala yang besar.

PKS AGC merangkumi perlindungan semua bentuk maklumat sama ada maklumat elektronik atau bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bertujuan untuk menjamin keselamatan dan ketersediaan maklumat kepada semua Pengguna, Pembekal dan Pihak Ketiga yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a) Kerahsiaan

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

10.0 BIDANG KAWALAN

Sebagai mendokong pematuhan PKS AGC bagi mengelakkan sebarang bentuk pelanggaran ke atasnya, bidang-bidang keselamatan siber yang berkaitan dinyatakan dengan jelas sebagai panduan/pembudayaan/ ikutan/ pemahaman. Terdapat 14 bidang keselamatan yang merujuk kepada Annex A piawaian ISO/IEC 27001:2022 Information Security Management Systems. 14 bidang tersebut adalah seperti Jadual 2:14 Bidang Kawalan Keselamatan Siber AGC.

Jadual 2: 16 Bidang Kawalan Keselamatan Siber AGC

BIDANG	TAJUK	BILANGAN KAWALAN
01	Dasar Keselamatan Maklumat	4
02	Organisasi Keselamatan Maklumat	15
03	Keselamatan Sumber Manusia	3
04	Pengurusan Aset	6
05	Kawalan Capaian/Akses	13
06	Kriptografi	4
07	Keselamatan Fizikal dan Persekitaran	16
08	Keselamatan Operasi	21
09	Keselamatan Komunikasi	9
10	Pemerolehan, Pembangunan Dan Penyelenggaraan Sistem Aplikasi	10
11	Hubungan Pembekal	5
12	Pengurusan Pengendalian Insiden Keselamatan Siber	2

BIDANG	TAJUK	BILANGAN KAWALAN
13	Pengurusan Kesinambungan Perkhidmatan	1
14	Pematuhan	5
15	Risikan Ancaman *(Threat Intelligence)*	1
16	Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*	1

Seterusnya setiap bidang kawalan keselamatan siber ini diterangkan secara lebih terperinci.

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 01:
DASAR KESELAMATAN MAKLUMAT

BIDANG 01: DASAR KESELAMATAN MAKLUMAT

0101 Polisi Keselamatan Siber AGC

Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan AGC dan perundangan yang berkaitan.

010101 Pelaksanaan PKS AGC	**Tanggungjawab**
Pelaksanaan dasar ini akan dijalankan dengan arahan Ketua Pengarah (KP) AGC.	KP

010102 Penyebaran/Hebahan PKS AGC	**Tanggungjawab**
PKS ini perlu dihebahkan kepada semua Pengguna, Pembekal dan Pihak Ketiga dari semasa ke semasa yang menggunakan aset ICT dan ruang siber di AGC.	STM

010103 Pematuhan dan Pengecualian PKS AGC	**Tanggungjawab**
PKS AGC perlu dipatuhi dan terpakai kepada semua Pengguna, Pembekal dan Pihak Ketiga. Tiada pengecualian bagi pematuhan PKS AGC.	Pengguna, Pembekal dan Pihak Ketiga

010104 Penyelenggaraan PKS AGC	**Tanggungjawab**
PKS AGC adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi,aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. PKS AGC hendaklah dikaji semula dengan kekerapan sekurang-kurangnya sekali dalam dua (2) tahun atau mengikut keperluan. Berikut adalah Prosedur Penyelenggaraan PKS AGC: (a) Mengenal pasti dan menentukan pindaan yang diperlukan; (b) Mengemukakan cadangan pindaan yang telah diselaras kepada JKSP ISMS AGC; (c) Mengemukakan cadangan pindaan secara bertulis untuk mendapat kelulusan Mesyuarat JPICT AGC; (d) Meminda dokumen PKS kepada versi baharu setelah pindaan diluluskan; dan (e) Memaklumkan pemakaian/penguatkuasaan PKS versi terkini kepada Pengguna, Pembekal dan Pihak Ketiga.	Ahli Jawatankuasa Kajian Semula Pengurusan (JKSP) ISMS AGC

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 02:
ORGANISASI KESELAMATAN MAKLUMAT

BIDANG 02: ORGANISASI KESELAMATAN MAKLUMAT

0201 Infrastruktur Organisasi Dalaman

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS AGC.

020101 Ketua Pengarah (KP) AGC	**Tanggungjawab**
Peranan dan tanggungjawab KP adalah seperti berikut: (a) Menentukan halatuju dan strategi pelaksanaan keselamatan siber AGC; (b) Memastikan semua keperluan organisasi (contoh: sumber kewangan, sumber manusia dan sumber perlindungan keselamatan) adalah mencukupi; (c) Memastikan penilaian risiko keselamatan siber dilaksanakan seperti yang ditetapkan di dalam PKS AGC; (d) Memastikan program keselamatan siber dilaksanakan; (e) Memastikan perancangan, penyelarasan dan penyeragaman pelaksanaan program/projek-projek keselamatan siber AGC supaya selaras dengan **Pelan Strategik Pendigitalan (PSP) AGC** yang sedang berkuatkuasa; dan (f) Melantik CDO AGC dan ICTSO AGC.	KP
020102 Ketua Pegawai Digital (CDO) AGC	**Tanggungjawab**
Timbalan Ketua Pengarah (Pembangunan) AGC ialah CDO AGC yang dilantik oleh KP. Peranan dan tanggungjawab CDO AGC adalah seperti berikut: (a) Meneraju inisiatif pendigitalan di Kementerian/Agensi melalui penggunaan data, analisis dan teknologi digital; (b) Mewujudkan budaya berpacukan data dalam sektor awam yang mengamalkan pendekatan *principle-based* melalui penggunaan data dan teknologi digital; (c) Mentransformasi penyampaian perkhidmatan digital di Kementerian/Agensi berfokuskan pengalaman pelanggan (*customer experience*) yang berteraskan konsep *Whole-of-Government* melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baru muncul; (d) Menilai, menyelaras, memperaku keperluan perkhidmatan digital, *Technical Service Design* dan bajet pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan;	CDO AGC

(e) Meneraju perubahan melalui Penjajaran Pelan Strategik Pendigitalan (PSP) Kementerian/Negeri/Agensi dengan: i. Memastikan PSP Agensi selari dengan PSP Sektor Awam dan Pengurusan Risiko dan Pelan Pengurusan Perubahan; ii. Memastikan *blueprint Enterprise Architecture* (EA) agensi tersedia; dan iii. Memantapkan struktur tadbir urus pendigitalan agensi & menyelaras penggunaan dasar, standard dan amalan terbaik global. (f) Melaporkan pelaksanaan dan kemajuan transformasi pendigitatan kepada YBhg. Ketua Setiausaha Negara sebagai Pengerusi Kluster Kerajaan di bawah Majlis Ekonomi Digital dan 41R Negara melalui sekretariat kluster kerajaan.	
020103 Ketua Pegawai Keselamatan (KPK) AGC	**Tanggungjawab**
Peranan dan tanggungjawab KPK AGC adalah seperti berikut: (a) Membantu melaksana urusan pergerakan kunci-kunci bangunan peringkat kementerian; (b) Membantu melaksana hal ehwal keselamatan di dalam peringkat kementerian; (c) Melaksanakan pemeriksaan operasi keselamatan dan kesihatan bersama jabatan lain di peringkat kementerian; (d) Melaksanakan dan bekerjasama dengan pihak berkuasa bagi keselamatan dan ketenteraman awam di kementerian ; dan (e) Menyediakan laporan ringkas jika ada melibatkan keselamatan fizikal, personel dan dokumen untuk diambil tindakan oleh pihak berkenaan.	KPK AGC

020104 Jawatankuasa Pemandu ICT (JPICT) AGC	Tanggungjawab
Keahlian JPICT AGC adalah terdiri daripada: <u>Pengerusi:</u> Peguam Negara atau Pegawai yang diturunkan kuasa <u>Ahli-ahli:</u> i. Ketua Pegawai Maklumat (CIO); ii. Ketua/Pengarah Bahagian; iii. Timbalan Pengarah Bahagian Pengurusan (Seksyen Teknologi Maklumat); iv. Pegawai Keselamatan ICT (ICTSO); v. Ketua Unit Audit Dalam (UAD); vi. Pegawai Perhubungan Awam; dan vii. Lain-lain ahli yang berkaitan. <u>Urus Setia:</u> Seksyen Teknologi Maklumat (STM) AGC. Peranan dan tanggungjawab JPICT AGC adalah seperti berikut: (a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT AGC; (b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT AGC; (c) Memantau pelaksanaan pensijilan ISMS AGC; (d) Memantau status kemajuan ISMS; (e) Meluluskan Polisi Keselamatan Siber (PKS) AGC; (f) Meluluskan Skop ISMS; dan (g) Meluluskan Tadbir Urus ISMS.	JPICT AGC
020105 Organisasi Pensijilan Sistem Pengurusan Keselamatan Maklumat (ISMS) AGC	**Tanggungjawab**
Struktur organisasi ISMS AGC melibatkan Jawatankuasa Pemandu ICT (JPICT), Jawatankuasa Kajian Semula Pengurusan ISMS, dan Jawatankuasa Pelaksana ISMS yang turut sama dibantu oleh Pasukan Penyelaras ISMS. Di samping itu, tadbir urus ISMS turut melibatkan kumpulan audit ISMS yang terdiri daripada Audit Dalam dan Audit Pensijilan ISMS. Struktur organisasi ISMS adalah seperti yang telah didokumenkan di dalam Manual ISMS AGC (AGC-ISMS-P1-002).	Jawatankuasa ISMS AGC

020106 Koordinator Pengurusan Kesinambungan Perkhidmatan (PKP) AGC	Tanggungjawab
Koordinator PKP AGC ialah pegawai yang dilantik oleh KP. Peranan dan tanggungjawab Koordinator PKP AGC adalah seperti berikut: (a) Bertindak sebagai pegawai perhubungan (single point of contact) bagi aktiviti pemulihan bencana dan mengetuai pelaksanaan aktiviti pemulihan bencana; (b) Memastikan ujian simulasi pemulihan bencana dijalankan mengikut jadual atau mengikut perancangan yang telah dipersetujui; (c) Mengurus penyediaan laporan ujian (post-mortem) dan melaksanakan penambahbaikan dokumen PKP; dan (d) Menyediakan dan melaksanakan penambahbaikan dokumen PKP.	Koordinator PKP AGC
020107 Pegawai Keselamatan ICT (ICTSO) AGC	**Tanggungjawab**
ICTSO bagi AGC ialah Pegawai Teknologi Maklumat yang dilantik oleh KP. ICTSO merupakan ahli Pasukan CSIRT AGC. Peranan dan tanggungjawab ICTSO AGC adalah seperti berikut: (a) Mengkaji dan melaksanakan kawalan keselamatan siber selaras dengan keperluan AGC; (b) Menentukan kawalan akses pengguna terhadap aset ICT; (c) Melaporkan sebarang insiden atau penemuan mengenai keselamatan siber kepada Pengarah CSIRT; (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber; (e) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan (f) Menangani insiden keselamatan siber AGC.	ICTSO AGC
020108 Pasukan Cyber Security Incident Response Team (CSIRT) AGC	**Tanggungjawab**
Keahlian CSIRT AGC adalah terdiri daripada:	CSIRT AGC

<u>Pengarah CSIRT</u>: *Chief Digital Officer* (CDO) <u>Pengurus CERT:</u> Ketua Seksyen Teknologi Maklumat Bahagian Khidmat Pengurusan <u>Ahli CERT:</u> Bahagian yang terlibat Peranan dan tanggungjawab CERT AGC adalah seperti berikut: (a) Memantau, mengesan insiden, menerima, mengesahkan aduan insiden keselamatan siber dan mengenal pasti jenis insiden serta menilai impak insiden; (b) Merekod dan menjalankan siasatan awal; (c) Melaksanakan pengurusan dan pengendalian insiden serta mengambil tindakan awal; (d) Menjalankan penialaian serta mendambil tindakan pengukuhan supaya insiden baharu dapat dielakkan; (e) Melapor insiden kepada Jabatan Perdana Menteri dan NC4; (f) Menasihati agensi mengambil tindakan pemulihan dan pengukuhan; (g) Hebahan makluman dan amaran berkaitan insiden kepada kakitangan agensi; dan (h) Memastikan fail log disimpan sekurang-kurangnya enam bulan.	
020109 Pentadbir Sistem ICT	**Tanggungjawab**
Pentadbir Sistem ICT ialah pegawai AGC yang dipertanggungjawabkan berdasarkan skop tugasan masing-masing seperti menyelenggara sistem aplikasi, sistem aplikasi mudah alih dan laman web. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (i) Mengambil tindakan segera mengikut proses yang ditetapkan	Pemilik Sistem dan Pentadbir Sistem ICT AGC

apabila dimaklumkan perubahan pengguna ICT melibatkan urusan perkhidmatan atau berlaku perubahan dalam bidang kuasa; (j) Menentukan ketepatan dan kesempurnaan (integriti) sesuatu tahap capaian berdasarkan arahan Pemilik Sistem sebagaimana yang telah ditetapkan di dalam PKS AGC; (k) Memantau aktiviti capaian harian sistem/aplikasi pengguna; (l) Mengenal pasti aktiviti-aktiviti tidak normal seperti pengubahsuaian data tanpa kebenaran serta membatalkan atau memberhentikannya dengan serta-merta dan melaporkannya kepada PICT; (m) Menganalisis, menyimpan, melindungi dan membuat *backup* rekod jejak audit; dan (n) Menyediakan laporan mengenai aktiviti capaian secara berkala kepada Pemilik Sistem.	
020110 Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT	**Tanggungjawab**
Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT ialah pegawai AGC yang dipertanggungjawabkan untuk merancang, mengurus, memantau dan menyelenggara Pusat Data, Rangkaian dan Komunikasi ICT. Peranan dan tanggungjawab Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT adalah seperti berikut: (a) Memastikan kerahsiaan akaun pentadbir; (b) Merangka, melaksana dan menguatkuasakan polisi keselamatan siber merangkumi: i. Perlindungan serta perkongsian data dan maklumat; ii. Ancaman keselamatan siber; dan iii. Capaian rangkaian dan komunikasi ICT. (c) Memastikan semua aset di Pusat Data berfungsi dan beroperasi dengan sempurna; (d) Menyelia dan membuat proses *backup* dan *restore*; dan (e) Menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian dan komunikasi ICT dan memantau operasi serta prestasi rangkaian dan komunikasi ICT.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
020111 Pegawai Aset	**Tanggungjawab**

Pegawai Aset ialah pegawai AGC yang dilantik oleh KP selaku Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK) peringkat Jabatan yang bertanggungjawab menguruskan aset kerajaan berdasarkan pekeliling yang berkuatkuasa. Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: (a) Memastikan pengurusan aset Kerajaan dijalankan selaras dengan peraturan yang ditetapkan dan pekeliling yang berkuatkuasa; (b) Memastikan penerimaan aset Kerajaan dilaksanakan oleh pegawai yang dilantik secara bertulis oleh KP selaku Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK); (c) Memastikan semua aset Kerajaan yang diterima, didaftarkan dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; (d) Memastikan semua aset Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan/Peminjaman Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Jabatan di AGC; (e) Memastikan Daftar Aset dikemas kini apabila berlaku penambahan/penggantian/penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan, pindahan dan hapus kira; (f) Memastikan semua aset Kerajaan diberi tanda pengenalan dengan cara melabel/mengecat/mencetak timbul (emboss) tanda Hak Kerajaan Malaysia dan nama AGC di tempat yang mudah dilihat dan sesuai pada aset berkenaan; (g) Memastikan semua aset Kerajaan dilabelkan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; (h) Memastikan senarai daftar induk aset Kerajaan disediakan; (i) Memastikan senarai aset Kerajaan mengikut lokasi disediakan berdasarkan format Senarai Aset Alih Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi; (j) Memastikan setiap kerosakan aset Kerajaan dilaporkan; (k) Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset Kerajaan; (l) Merancang, memantau dan memastikan pemeriksaan aset Kerajaan dilaksanakan ke atas keseluruhan aset alih Kerajaan sekurang-kurangnya sekali setahun; dan (m) Memastikan setiap kes kehilangan aset Kerajaan dilaporkan dan diuruskan dengan teratur.	KP dan Pegawai Aset AGC
020112 Unit Komunikasi Korporat	**Tanggungjawab**

Unit Komunikasi Korporat ialah pegawai AGC yang menguruskan hal ehwal media sosial. Peranan dan tanggungjawab Unit Komunikasi Korporat adalah seperti berikut: (a) Memaklumkan tujuan pewujudan media sosial dan mendapat perakuan mematuhi syarat-syarat sebagai ahli kumpulan media sosial tersebut; (b) Sentiasa peka terhadap peraturan atau syarat-syarat yang ditetapkan oleh penyedia platform; (c) Melaksanakan pemantauan terhadap pengguna untuk memastikan pengguna sentiasa mematuhi syarat-syarat serta garis panduan keselamatan media sosial yang telah ditetapkan; dan (d) Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuatkuasa.	Unit Komunikasi Korporat AGC
020113 Pengguna	**Tanggungjawab**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami, dan mematuhi PKS AGC; (b) Mengetahui dan memahami implikasi keselamatan siber akibat daripada tindakannya; (c) Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan) berdasarkan Arahan Keselamatan Kerajaan yang sedang berkuatkuasa; (d) Melaksanakan dan mematuhi prinsip-prinsip PKS AGC serta menjaga kerahsiaan maklumat AGC; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan (g) Menandatangani Surat Akuan Pematuhan PKS AGC seperti **LAMPIRAN 1** melalui Sistem Pematuhan PKS AGC.	Pengguna
0202 Pembekal dan Pihak Ketiga **Objektif:** Menjamin keselamatan semua aset ICT yang digunakan oleh Pembekal dan Pihak Ketiga. Contoh: Pakar Runding.	
020201 Keperluan Keselamatan Kontrak dengan Pembekal dan Pihak Ketiga	**Tanggungjawab**

Ini bertujuan memastikan penggunaan maklumat dan kemudahan pemprosesan maklumat di AGC dengan Pembekal dan Pihak Ketiga dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membaca, memahami dan mematuhi PKS AGC; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada Pembekal dan Pihak Ketiga; (d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan Pembekal dan Pihak Ketiga. Perkara-perkara berikut hendaklah dilaksanakan dan dipatuhi tertakluk kepada skop/ bidang tugas yang berkaitan: i. Pematuhan PKS AGC; ii. Tapisan Keselamatan melalui sistem eVetting CGSO; dan iii. Perakuan Akta Rahsia Rasmi 1972. (e) Akses kepada aset ICT AGC perlu berlandaskan kepada perjanjian kontrak perkhidmatan yang telah dipersetujui dengan Pembekal dan Pihak Ketiga; dan (f) Menandatangani Surat Akuan Pematuhan PKS AGC seperti **LAMPIRAN 1**.	CDO, ICTSO, PICT, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC, Pembekal dan Pihak Ketiga

0203 Keselamatan Maklumat Dalam Pengurusan Projek

Objektif: Mengenal pasti risiko keselamatan maklumat bagi mengawal dan menjamin keselamatan maklumat dalam pengurusan projek.

020301 Pengurusan Projek ICT dan Keselamatan Maklumat	**Tanggungjawab**
Pengurusan Projek ICT merupakan satu pengurusan proses dan prosedur dalam satu tempoh masa, sumber dan tahap kualiti yang ditetapkan bagi menghasilkan satu atau lebih produk ICT. Keselamatan maklumat perlu diambil kira dalam pengurusan projek bagi melindungi maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	CDO, PICT, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC, Pembekal dan Pihak Ketiga

(a) Memastikan objektif keselamatan maklumat dimasukkan di dalam objektif projek; (b) Melaksanakan penilaian risiko keselamatan maklumat hendaklah di peringkat awal pelaksanaan projek bagi menentukan kaedah kawalan yang bersesuaian; (c) Memastikan keselamatan maklumat bagi setiap fasa metodologi pembangunan projek dilaksanakan; dan (d) Memastikan implikasi keselamatan maklumat bagi semua projek ditangani secara teratur dan berkesan.	

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 03:
KESELAMATAN SUMBER MANUSIA

BIDANG 03: KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia dalam Tugas Rasmi Harian	
Objektif: Memastikan Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT dan ruang siber. Pengguna, Pembekal dan Pihak Ketiga hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
030101 Sebelum Perkhidmatan	**Tanggungjawab**
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT **sebelum perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis sebelum perkhidmatan; (b) Menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; (c) Pengguna perlu mengisi secara dalam talian Akuan Pematuhan PKS AGC; (d) Pengguna perlu menandatangani Perakuan Akta Rahsia Rasmi 1972; (e) Pembekal dan Pihak Ketiga perlu menandatangani Surat Akuan Pematuhan PKS AGC seperti LAMPIRAN 1; (f) Pembekal dan Pihak Ketiga perlu menandatangani Perakuan Akta Rahsia Rasmi 1972; dan (g) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna, Pembekal dan Pihak Ketiga
030102 Dalam Perkhidmatan	**Tanggungjawab**
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT **dalam perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan	Pengguna, Pembekal dan Pihak Ketiga

aset ICT secara bertulis semasa perkhidmatan; (b) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan keselamatan aset ICT diurus berdasarkan prosedur dan peraturan yang ditetapkan oleh AGC; (c) Pengguna perlu memastikan program kesedaran yang berkaitan mengenai pengurusan keselamatan aset ICT dihadiri secara berterusan dan berusaha meningkatkan kemahiran keselamatan siber; (d) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan sentiasa mempunyai kesedaran berkenaan kepentingan menjaga rahsia Kerajaan dalam urusan kerja harian; (e) Pengguna perlu mengambil maklum mengenai tindakan disiplin dan/atau undang-undang yang akan dikenakan sekiranya berlaku perlanggaran dengan prosedur dan peraturan ditetapkan oleh AGC; dan (f) Pengguna perlu memantapkan pengetahuan berkaitan dengan penggunaan aset ICT melalui medium kursus, latihan teknikal dan medium yang bersesuaian bagi memastikan setiap kemudahan ICT digunakan dengan tujuan dan cara yang betul demi menjamin kepentingan keselamatan siber.	
030103 Bertukar atau Tamat Perkhidmatan	**Tanggungjawab**
Memastikan semua Pengguna, Pembekal dan Pihak Ketiga yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT sebelum **bertukar atau tamat perkhidmatan** agar meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT secara bertulis selepas perkhidmatan; (b) Pengguna perlu memastikan semua aset ICT dikembalikan kepada AGC mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (c) Pengguna, Pembekal dan Pihak Ketiga perlu memastikan kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan atau ditarik balik dengan serta-merta mengikut peraturan yang ditetapkan oleh AGC; (d) Pengguna, Pembekal dan Pihak Ketiga perlu melaksanakan perakuan bagi melupuskan semua maklumat terperingkat dalam simpanan secara selamat; dan (e) Menandatangani Borang Pengesahan Pegawai Bertukar Keluar Atau Tamat Perkhidmatan Di AGC seperti **LAMPIRAN 2**.	Pengguna, Pembekal dan Pihak Ketiga

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 04:
PENGURUSAN ASET

BIDANG 04: PENGURUSAN ASET

0401 Akauntabiliti Aset

Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset AGC.

040101 Aset ICT	**Tanggungjawab**
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh Pengguna masing-masing. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT perolehan secara pembelian dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa ke dalam sistem pengurusan aset berdasarkan pekeliling yang sedang berkuatkuasa; (b) Memastikan semua aset perolehan secara sewaan dikenal pasti dan maklumat aset direkodkan serta dikemaskini dari semasa ke semasa; (c) Memastikan semua aset ICT diuruskan oleh Penyelaras ICT/Pegawai Aset dan dikendalikan oleh Pengguna yang dibenarkan sahaja; (d) Memastikan semua Pengguna mengesahkan penempatan aset ICT yang ditempatkan; (e) Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan; (f) Setiap Pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan (g) Memastikan semua aset ICT diagihkan kepada Pengguna mengikut piawaian dan garis panduan yang ditetapkan.	Pegawai Aset, Penyelaras ICT AGC dan Pengguna

0402 Pengelasan, Pengendalian dan Keselamatan Maklumat

Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

040201 Pengelasan Maklumat	**Tanggungjawab**
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau	Pegawai Pengelas

(d) Terhad.	
040202 Pelabelan Maklumat	**Tanggungjawab**
Maklumat hendaklah dilabelkan sewajarnya. Penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan Kerajaan yang sedang berkuatkuasa seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Pengguna
040203 Pengendalian Maklumat	**Tanggungjawab**
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi *standard*, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian terutama semasa aktiviti pengendalian maklumat terperingkat; (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; dan (h) Mewujudkan sandaran/ salinan pendua maklumat penting bagi mengurangkan risiko kehilangan dan kemusnahan serta memelihara kerahsiaan maklumat terperingkat.	Pengguna
040204 Keselamatan Maklumat	**Tanggungjawab**
Keselamatan maklumat penting bagi perlindungan data- dalam-penggunaan, data-dalam-pergerakan, data-dalam- simpanan dan menghalang ketirisan data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna

(a) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh Pengguna yang dibenarkan sahaja; (b) Menggunakan teknologi enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; dan (c) Semua maklumat terperingkat hendaklah dihapuskan mengikut prosedur pelupusan semasa yang sedang berkuatkuasa.	
040205 *Data Masking*	**Tanggungjawab**
Data Masking ialah teknik yang digunakan untuk mencipta versi data yang kelihatan secara struktur seperti yang asal tetapi menyembunyikan maklumat sensitif. Versi dengan maklumat bertopeng kemudiannya boleh digunakan untuk pelbagai tujuan, seperti latihan pengguna atau ujian perisian. Objektif utama menyembunyikan data adalah untuk mencipta pengganti berfungsi yang tidak mendedahkan data sebenar. Data yang sepatutnya ditutup ialah: • *Personal Identifiable Information* (PII) ○ Data yang boleh digunakan untuk mengenal pasti individu tertentu. Ini termasuk maklumat seperti nama penuh, nombor pasport, nombor lesen memandu dan nombor keselamatan sosial.	Pengguna
0403 ICT Hijau Kerajaan (Government Green ICT) **Objektif:** Memastikan aset ICT mematuhi ciri-ciri ICT Hijau Kerajaan.	
040301 Pengurusan Aset ICT	**Tanggungjawab**
Amalan penggunaan peralatan ICT ke arah ICT Hijau bagi mengurangkan penggunaan tenaga. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perolehan aset ICT mengambil kira pematuhan elemen ICT Hijau Kerajaan; (b) Memastikan kerja-kerja seharian mengguna pakai prinsip pengurangan (reduce), penggunaan semula (reuse) dan kitar semula (recycle); (c) Memastikan sistem pengurusan kuasa (power management) aset ICT diaktifkan; dan (d) Memastikan peralatan ICT dilupuskan dan penggunaan semula	PICT, Pentadbir Peralatan ICT AGC dan Pengguna

alat ganti mengikut prosedur yang mengambil kira pemuliharaan alam sekitar.	

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 05:
KAWALAN CAPAIAN/AKSES

BIDANG 05: KAWALAN CAPAIAN/AKSES

0501 Dasar Kawalan Capaian/Akses **Objektif:** Peraturan kawalan capaian hendaklah mengambil kira faktor **had** capaian dan **hak** capaian (authorization) ke atas data dan maklumat serta proses capaian maklumat.	
050101 Keperluan Kawalan Capaian/Akses	**Tanggungjawab**
Kawalan Capaian/Akses merupakan pendekatan untuk mengehadkan capaian sistem kepada Pengguna yang berdaftar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan Pengguna; (b) Melaksanakan kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Melaksanakan keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Melaksanakan kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir Peralatan ICT AGC dan Pengguna
0502 Pengurusan Capaian/Akses Pengguna **Objektif:** Mengawal capaian pengguna ke atas aset ICT AGC.	
050201 Akaun Pengguna	**Tanggungjawab**
Setiap Pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Akaun Pengguna diwujudkan bagi mengenalpasti Pengguna dan aktiviti yang dilakukan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akaun yang diperuntukkan sahaja boleh digunakan; (b) Akaun Pengguna mestilah unik; (c) Pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya; (d) Akaun Pengguna akan dibeku atau ditamatkan atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi 90 hari; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	Pemilik Sistem, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC dan Pengguna

(e) Sebarang perubahan tahap akses bagi Pengguna hendaklah mendapat kelulusan daripada Pemilik Sistem; dan (f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.	
050202 Hak Capaian/ Akses	**Tanggungjawab**
Pengurusan dan pemantauan hak capaian terhadap akaun- akaun dan sistem aplikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas; dan (b) Hak capaian Pengguna diberi berdasarkan peranan dan tanggungjawab Pengguna.	Pemilik Sistem, Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT AGC dan Pengguna
050203 Pengurusan Kata Laluan	**Tanggungjawab**
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta memastikan keselamatan kata laluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Kata laluan hendaklah 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 apabila meninggalkan komputer melebihi 10 minit; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (h) Kata laluan hendaklah ditukar dalam tempoh yang ditetapkan; dan (i) Sistem aplikasi yang dibangunkan digalakkan mempunyai kemudahan menukar kata laluan oleh Pengguna.	Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT AGC dan Pengguna
050204 *Clear Desk* dan *Clear Screen*	**Tanggungjawab**

Clear Desk dan *Clear Screen* merupakan amalan yang digalakkan bagi menjaga keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna
050205 Capaian/Akses Pengguna	**Tanggungjawab**
Capaian/Akses Pengguna melibatkan aktiviti muat naik, muat turun dan penggunaan untuk tujuan yang dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan; dan (b) Pengguna adalah DILARANG melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen serta 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, jenayah atau pernyataan berbentuk hasutan tanpa kebenaran berbuat demikian.	Pengguna
0503 Kawalan Capaian/ Akses Rangkaian Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
050301 Capaian/Akses Rangkaian	**Tanggungjawab**
Kawalan capaian perkhidmatan rangkaian adalah bagi menjamin keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menempatkan atau memasang antara muka yang bersesuaian antara rangkaian AGC, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian	ICTSO dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

penggunaannya; (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; (d) Mentadbir dan mengawal capaian Pengguna jarak jauh (remote user) dengan kebenaran bertulis; (e) Mentadbir dan mengawal rangkaian yang dikongsi (shared networks), terutama sekali yang keluar daripada rangkaian AGC; dan (f) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang perkakasan ICT yang bersesuaian di rangkaian AGC.	
050302 Capaian/ Akses Internet	**Tanggungjawab**
Capaian internet bagi urusan rasmi membolehkan Pengguna berhubung dan mencapai maklumat dalam persekitaran yang selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pemantauan secara berterusan dilakukan bagi memastikan penggunaannya hanya untuk capaian yang dibenarkan sahaja; (b) Penguatkuasaan *Content Filtering* hendaklah dilaksanakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Pengawalan penggunaan bandwidth hendaklah dilaksanakan bagi penggunaan bandwidth yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja; (e) Pengguna hanya dibenarkan memuat turun perisian yang sah dan berdaftar; (f) Perolehan/ pembelian dan penggunaan broadband bergantung kepada justifikasi atau keperluan dan perlu mendapat kelulusan Pengurusan AGC; dan (g) Penggunaan kemudahan internet peribadi di pejabat seperti modem, hotspot dan sebagainya untuk tujuan sambungan ke Internet adalah perlu mendapat kelulusan jika melibatkan sambungan ke rangkaian AGC.	ICTSO, PICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC dan Pengguna
0504 Kawalan Capaian/Akses Sistem Pengoperasian **Objektif:** Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
050401 Capaian/ Akses Sistem Pengoperasian	**Tanggungjawab**
Sistem Pengoperasian membolehkan Kawalan Capaian Sistem Pengoperasian bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sumber sistem	Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan

<table>
<tr><td>komputer.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Mengawal capaian ke atas sistem pengoperasian menggunakan mekanisme log masuk 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 perisian;
(d) Mengehadkan tempoh penggunaan dan/atau sambungan ke sesebuah aplikasi berisiko tinggi;
(e) Mengesahkan Pengguna yang dibenarkan selaras dengan peraturan AGC; dan
(f) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian.</td><td>Komunikasi ICT AGC dan Pengguna</td></tr>
<tr><td colspan="2">0505 Kawalan Capaian/ Akses Sistem Aplikasi dan Maklumat
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.</td></tr>
<tr><td>050501 Capaian/ Akses Sistem Aplikasi dan Maklumat</td><td>Tanggungjawab</td></tr>
<tr><td>Capaian sistem aplikasi dan maklumat adalah terhad kepada Pengguna dan tujuan yang dibenarkan sahaja.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Penggunaan sistem aplikasi yang dibenarkan adalah mengikut ketetapan kawalan capaian, tahap capaian dan keselamatan yang telah ditentukan;
(b) Memastikan jejak audit dan sistem log dilaksanakan bagi setiap aktiviti capaian sistem aplikasi dan maklumat;
(c) Mengehadkan capaian sistem aplikasi dan maklumat kepada lima (5) kali percubaan. Sekiranya gagal, pengguna dan pentadbir sistem perlu menetapkan semula kata laluan;
(d) Mengawal capaian ke atas sistem aplikasi dan maklumat menggunakan prosedur log masuk yang selamat, kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;
(e) Capaian sistem aplikasi dan maklumat melalui capaian internet adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan
(f) Capaian kepada sistem aplikasi di AGC hendaklah mempunyai ciri-ciri keselamatan (contoh penggunaan Secure Socket Layer (SSL): https).</td><td>Pentadbir Sistem ICT AGC dan Pengguna</td></tr>
<tr><td colspan="2">0506 Peralatan Mudah Alih dan Kerja Jarak Jauh
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.</td></tr>
</table>

050601 Kawalan Peralatan Mudah Alih	**Tanggungjawab**
Peralatan mudah alih yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik perlu diberi kawalan perlindungan bagi memastikan keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua Pengguna bertanggungjawab sepenuhnya terhadap pengurusan dan kawalan keselamatan setiap peralatan mudah alih yang dibekalkan; (b) Rekod penggunaan peralatan mudah alih hendaklah diwujudkan, dikemaskini dan diperiksa; (c) Memastikan peralatan mudah alih dihindari daripada sebarang ancaman, keselamatan maklumat seperti pendedahan, kecurian, pengubahsuaian dan pemalsuan; (d) Peralatan mudah alih tidak disimpan di dalam kenderaan tanpa pengawasan, di tempat-tempat awam dan premis/ kawasan yang tidak selamat; dan (e) Peralatan mudah alih yang didapati hilang hendaklah diuruskan berdasarkan kepada pekeliling semasa yang berkuatkuasa.	Pegawai Aset AGC dan Pengguna
050602 Kawalan Kemudahan Kerja Jarak Jauh	**Tanggungjawab**
Kawalan Kemudahan Kerja Jarak Jauh adalah bagi memastikan tiada berlakunya kehilangan peralatan, pendedahan maklumat dan capaian tidak sah dan salah guna kemudahan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk melindungi dari risiko penyalahgunaan peralatan mudah alih dan kemudahan komunikasi; (b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan (c) Untuk capaian dari luar rangkaian AGC ke rangkaian MyGov*Net dengan menggunakan Virtual Private Network (VPN) perlu melalui permohonan kepada STM.	Pengguna
0507 Bring Your Own Device (BYOD) **Objektif:** Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD di AGC.	
050701 Keperluan dan Kawalan Penggunaan BYOD	**Tanggungjawab**
Penggunaan BYOD yang disambungkan kepada rangkaian AGC	Pengguna

sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada keperluan dan kawalan penggunaan BYOD. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat; (b) Pengguna perlu mengetahui peraturan-peraturan yang telah ditetapkan apabila menggunakan BYOD; (c) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada penggunaan BYOD; (d) Pendaftaran ke atas peralatan mudah alih; (e) Keperluan ke atas perlindungan secara fizikal; (f) Kawalan ke atas pemasangan perisian peralatan mudah alih; (g) Kawalan ke atas versi dan *patches* perisian; (h) Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; (i) Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptograf; dan (j) Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	

BIDANG 06:
KRIPTOGRAFI

BIDANG 06: KRIPTOGRAFI

0601 Kawalan Kriptografi **Objektif:** Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Enkripsi	**Tanggungjawab**
Enkripsi/ penyulitan digunakan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap maklumat terperingkat hendaklah disulitkan; (b) Untuk mengendalikan Maklumat Rasmi penggunaan Produk Kriptografi Terpercaya adalah digalakkan; dan (c) Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan dan dibuat enkripsi.	Pemilik Sistem, Pentadbir Sistem ICT AGC dan Pengguna
060102 Tandatangan Digital	**Tanggungjawab**
Penggunaan tandatangan digital adalah mengikut keperluan pelaksanaan dan melibatkan Sijil Digital. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan tandatangan digital adalah dimestikan kepada pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; dan (b) Sijil Digital yang digunakan hendaklah diperoleh daripada Pihak Berkuasa Pemerakuan Berlesen sahaja.	Pemilik Sistem, Pentadbir Sistem ICT AGC dan Pengguna
060103 Pengurusan Infrastruktur Kunci Awam (PKI)	**Tanggungjawab**
PKI merupakan teknologi berasaskan sijil digital yang dapat membantu organisasi menggunakan tandatangan digital, enkripsi dan pengesahan identiti antara manusia, sistem dan peranti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan	Pentadbir Sistem ICT AGC dan Pengguna

dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; (b) Kunci persendirian mesti disimpan dengan selamat dan hanya digunakan oleh entiti yang memilikinya sahaja bagi tujuan nyahsulit atau mewujudkan tandatangan digital. Kunci awam tersedia bagi ahli kumpulan yang menggunakan enkripsi bagi menentusah tandatangan digital yang diterima; dan (c) Pengurusan sijil digital pelayan *Secure Socket Layer* (SSL) hendaklah dilakukan bagi mengelakkan sebarang capaian, kecurian atau digunakan oleh pihak lain.	
060104 Sijil Digital	**Tanggungjawab**
Sijil Digital adalah sijil yang dikeluarkan oleh Pihak Berkuasa Pemerakuan Berlesen (CA) untuk mengesahkan tanpa penafian identiti pengguna atau pelayan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan sijil digital hendaklah dilaksanakan dalam capaian aplikasi Kerajaan Elektronik yang ditetapkan; (b) Sijil Digital terdapat dalam tiga (3) medium iaitu *Token, Roaming dan SoftCert;* dan (c) Semua akses dan peranan Pengguna yang bertukar keluar/ bersara hendaklah disekat dan ditamatkan sijil digitalnya oleh Pentadbir Sistem ICT.	Pentadbir Sistem ICT AGC dan Pengguna

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 07:
KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 07: KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan dan Persekitaran

Objektif: Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, kerosakan, ancaman, gangguan persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, kecurian atau kemalangan serta akses yang tidak dibenarkan.

070101 Kawalan Kawasan	Tanggungjawab
Kawalan Kawasan bertujuan menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan dan lain- lain) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Melindungi kawasan terhad melalui kawalan-kawalan tertentu seperti memasang alat penggera, kamera litar tertutup atau EMS sekiranya berkaitan; (d) Mengehadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan ruang menunggu atau ruang kerja untuk Pihak Ketiga (jika perlu); (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam ruang dan bilik pejabat serta kemudahan yang disediakan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk warga yang bekerja di dalam kawasan terperingkat; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	PK AGC

070102 Kawalan Persekitaran	Tanggungjawab
Kawalan persekitaran bertujuan menghindar kerosakan dan capaian terhadap peralatan ICT dan peralatan rangkaian bagi keselamatan maklumat agensi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan susun atur semua aset ICT di Pusat Data adalah teratur dan kemas; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan peralatan perlindungan keselamatan yang bersesuaian dan dibenarkan seperti alat pengesan kebakaran, alat pencegah kebakaran dan pintu kecemasan; (c) Semua bahan mudah terbakar, cecair, bahan atau peralatan lain yang boleh merosakkan peralatan ICT hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT; (d) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT; (e) Memastikan akses kepada saluran riser sentiasa dikunci; (f) Memastikan peralatan rangkaian seperti switch, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (g) Memastikan pegawai yang bertanggungjawab menyimpan semua kunci yang berkenaan dapat dihubungi apabila keadaan memerlukan berbuat demikian; (h) Insiden kecemasan persekitaran mesti dilaporkan; dan (i) Merancang dan menyertai latihan kecemasan bencana yang diadakan di AGC.	ICTSO, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC dan Pengguna
070103 Kawalan Masuk Fizikal	**Tanggungjawab**
Kawalan masuk fizikal bertujuan mengawal akses oleh pihak-pihak Pengguna, Pembekal dan Pihak Ketiga bagi keselamatan maklumat organisasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pas keselamatan hendaklah dipakai sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada AGC apabila Pengguna berhenti, bersara atau berpindah keluar; (c) Pihak Ketiga hendaklah menyerahkan semula pas pelawat kepada AGC apabila urusan selesai atau tamat kontrak; (d) Pas pelawat hendaklah diambil di kaunter masuk. Pas ini	PK AGC Pengguna, Pembekal dan Pihak Ketiga

hendaklah dikembalikan semula selepas tamat lawatan; dan (e) Kehilangan pas keselamatan/pelawat mestilah dilaporkan dengan segera kepada Pegawai Keselamatan AGC.	
070104 Kawasan Larangan	**Tanggungjawab**
Kawasan Larangan dilaksanakan untuk melindungi aset ICT. Kawasan larangan ICT di AGC adalah Pusat Data/Bilik Server/Stor ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Tanda kawasan larangan hendaklah dipamerkan; (b) Buku log keluar/masuk Pusat Data sentiasa dipantau dan diselenggara; (c) Pihak Ketiga dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal; (d) Pihak Ketiga hendaklah diiringi dan dipantau sepanjang masa oleh pegawai yang diberi kebenaran untuk mengakses Pusat Data sehingga tugas di kawasan berkenaan selesai. Pihak Ketiga juga perlu mematuhi semua peraturan Pusat Data yang ditetapkan; dan (e) Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam Pusat Data kecuali dengan kebenaran Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC, Pembekal dan Pihak Ketiga
070105 Bekalan Kuasa	**Tanggungjawab**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan kuasa; (b) Peralatansokongan seperti UPS dan Genset boleh digunakan bagi perkhidmatan kritikal supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa, diuji dan diselenggara secara berjadual.	ICTSO dan PK AGC
070106 Kabel	**Tanggungjawab**

Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah. Perkara-perkara yang perlu dipatuhi 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.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
0702 Keselamatan Peralatan Objektif: Melindungi peralatan ICT AGC daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
070201 Peralatan ICT	**Tanggungjawab**
Pengguna yang diberikan peralatan ICT hendaklah menjaga dan bertanggungjawab sepenuhnya ke atas peralatan ICT tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. (b) Melaporkan sebarang kerosakan peralatan ICT melalui saluran yang ditetapkan; (c) Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran dan perubahan konfigurasi yang telah ditetapkan; (d) Dilarang sama sekali menambah, mengganti atau mengeluarkan sebarang perkakasan ICT yang telah ditetapkan; (e) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Peralatan ICT; (f) Bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (g) Memastikan perisian antivirus yang dibekalkan di komputer peribadi/komputer riba sentiasa aktif (*active*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan. Pengguna dilarang untuk menyahpasang (*uninstall*) antivirus yang telah dipasang (*installed*); (h) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (i) Semua peralatan sokongan ICT (aksesori) hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (j) Peralatan-peralatan kritikal perlu disokong oleh UPS;	Pegawai Aset, PICT, Pentadbir Peralatan ICT AGC dan Pengguna

(k) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (m) Peralatan ICT yang hendak dibawa keluar dari premis AGC hendaklah mematuhi peraturan yang telah ditetapkan; (n) Peralatan ICT yang hilang hendaklah dilaporkan kepada PICT dan Pegawai Aset AGC dengan segera; (o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (p) Pengguna tidak dibenarkan mengalih kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset AGC. Perpindahan peralatan ICT hendaklah mematuhi peraturan yang telah ditetapkan; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (s) Bertanggungjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (t) Memastikan semua peralatan ICT yang tidak digunakan dalam keadaan tutup (*off*) apabila meninggalkan pejabat; (u) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat; dan (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada PICT.	
070202 Media Storan	**Tanggungjawab**
Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian mengikut kategori maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC dan Pengguna

dan selamat; (e) Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang mempunyai ciri-ciri keselamatan dengan mengikut prosedur yang telah ditetapkan; (f) Mematuhi prosedur pengurusan media storan yang telah dikenal pasti termasuk akses, inventori, pergerakan, pelabelan serta backup dan restore; (g) Perkakasan backup hendaklah diletakkan di tempat yang terkawal; (h) Mengadakan salinan atau backup pada media storan kedua bagi tujuan keselamatan dan mengelakkan kehilangan data. Media storan kedua hendaklah disimpan di tempat yang selamat; (i) Semua maklumat dalam media storan yang hendak dilupuskan mestilah dihapuskan terlebih dahulu. Proses pelupusan hendaklah dilakukan dengan teratur dan selamat mengikut prosedur pelupusan; (j) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan (k) Sebarang kehilangan media storan yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.	
070203 Media Sijil Digital	**Tanggungjawab**
Sijil Digital terdapat dalam tiga (3) medium iaitu Token, *Roaming* dan *SoftCert.* Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media sijil digital daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian penggunaan token adalah tidak dibenarkan sama sekali; (d) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (e) Sebarang kehilangan media sijil digital yang berlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.	Pengguna
070204 Media Perisian	**Tanggungjawab**
Media perisian merupakan *disk*/media yang digunakan apabila perisian diedarkan.	Pentadbir Sistem ICT dan Pentadbir Pusat Data,

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan AGC; dan (b) Lesen perisian (*registration code, serials dan CD-keys*) perlu disimpan berasingan daripada *CD-ROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak.	Rangkaian dan Komunikasi ICT AGC
070205 Penyelenggaraan Peralatan ICT	**Tanggungjawab**
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT yang diselenggara hendaklah mengikut spesifikasi yang telah ditetapkan; (b) Memastikan peralatan ICT hanya boleh diselenggara oleh Pentadbir Peralatan ICT atau Pembekal atau Pihak Ketiga yang dibenarkan sahaja; (c) Penyelenggaraan melibatkan perkakasan ICT dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pentadbir Peralatan ICT AGC, Pengguna, Pembekal dan Pihak Ketiga
070206 Peralatan ICT Dibawa Keluar Dari Premis	**Tanggungjawab**
Peralatan ICT yang dibawa keluar dari premis AGC adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT termasuk perisian dan maklumat perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Kehilangan peralatan ICT perlu dilaporkan mengikut prosedur pengurusan aset yang ditetapkan.	Pentadbir Peralatan ICT AGC, Pengguna, Pembekal dan Pihak Ketiga
070207 Pemadaman Data dan Pelupusan Peralatan ICT	**Tanggungjawab**
Pemadaman Data dan Pelupusan melibatkan data dan peralatan ICT yang tidak digunakan, telah rosak, usang dan tidak boleh dibaiki yang dibekalkan.	Pegawai Aset AGC dan Pengguna

Terdapat banyak rekod dan dokumen yang perlu disediakan & diselenggara dalam bentuk kertas. Oleh itu, dokumen yang disimpan di atas kertas adalah penting untuk dirincihkan atau dimusnahkan mengikut dasar, supaya semua maklumat dilupuskan dengan betul, mengikut garis panduan AGC. Pelupusan dan pemusnahan dilakukan selepas kelulusan pengurus pelupusan. Pegawai hendaklah mengambil berat dan memastikan bukti yang digunakan oleh organisasi tidak dimusnahkan. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; (c) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut prosedur pelupusan semasa yang berkuat kuasa; dan (d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan. Contoh: CPU, RAM, *hardisk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan; dan iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dilupuskan.	
070208 Pindahan Peralatan ICT	**Tanggungjawab**
Pindahan melibatkan semua peralatan ICT yang masih berkeadaan baik. Peralatan ICT yang hendak dipindahkan mestilah mendapat kelulusan bertulis daripada Ketua Jabatan antara Bahagian/ Jabatan pemberi dan Bahagian/ Jabatan penerima. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT yang hendak dipindahkan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri	Pegawai Aset AGC dan Pengguna

keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir-butir pindahan dan mengemas kini rekod pindahan peralatan ICT; (c) Pindahan peralatan ICT hendakla dilakukan secara berpusat dan mengikut Tatacara Pengurusan Aset Alih Kerajaan yang sedang berkuatkuasa; dan (d) Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dipindahkan. Contoh: CPU, RAM, hardisk, motherboard dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan; dan iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dipindahkan.	

0703 Keselamatan Dokumen

Objektif: Melindungi maklumat AGC daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.

070301 Dokumen	**Tanggungjawab**
Dokumen mengandungi Maklumat Rasmi atau Maklumat Terperingkat hedaklah didaftar, dikelas (dikelaskan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad), dikelas semula dan dilupus dengan mematuhi peraturan yang sedang berkuat kuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen (termasuk pergerakan ke luar dari premis AGC) hendaklah dikawal dan direkodkan serta perlu mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan Kerajaan yang sedang berkuatkuasa; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa; dan (e) Penyimpanan maklumat rasmi di storan dalam talian diluar kawalan AGC adalah tidak dibenarkan.	Pengguna

BIDANG 08:
KESELAMATAN OPERASI

BIDANG 08: KESELAMATAN OPERASI

<table>
<tr><td colspan="2">0801 Pengurusan Prosedur Operasi

Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.</td></tr>
<tr><td>080101 Pengendalian Prosedur</td><td>Tanggungjawab</td></tr>
<tr><td>Prosedur adalah dasar yang mengatur pengoperasian sistem maklumat.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal;

(b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

(c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.</td><td>ICTSO,
PICT,
Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC</td></tr>
<tr><td>080102 Kawalan Perubahan</td><td>Tanggungjawab</td></tr>
<tr><td>Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Pemilik Sistem dan/ atau PICT dan/atau Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT terlebih dahulu;

(b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana perkakasan ICT hendaklah dikendalikan oleh Pentadbir Peralatan ICT dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;

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

(d) Semua aktiviti perubahan atau pengubahsuaian hendaklah</td><td>ICTSO,
Pemilik Sistem,
PICT,
Pentadbir Sistem ICT, Pentadbir Peralatan ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC</td></tr>
</table>

direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
080103 Pengasingan Tugas dan Tanggungjawab	**Tanggungjawab**
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab termasuk mewujud, memadam, mengemas kini, mengubah dan mengesahkan perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan, akses atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT daripada ralat, kebocoran maklumat terperingkat atau dimanipulasi; (b) Aset ICT yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (*production*). Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun sistem dan pelaksana operasi; dan (c) Pengasingan tugas bagi tugasan yang bersifat kritikal tidak boleh dilaksanakan oleh seorang individu sahaja atas kuasa tunggalnya dan hendaklah dikendalikan dalam tadbir urus yang bersesuaian.	PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
0802 Pengurusan Penyampaian Perkhidmatan Pembekal dan Pihak Ketiga **Objektif:** Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat serta penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan Pembekal dan Pihak Ketiga.	
080201 Perkhidmatan Penyampaian ICT	**Tanggungjawab**
Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal. Perkara-perkara yang mesti dipatuhi adalah seperti berikut:	PICT, Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT

(a) Memastikan definisi perkhidmatan kawalan keselamatan, tahap penyampaian dan penyelenggaraan yang terkandung dalam perjanjian dipatuhi, dilaksanakan oleh Pembekal dan Pihak Ketiga; (b) Memantau perkhidmatan dan menyemak laporan serta rekod yang dikemukakan oleh Pembekal dan Pihak Ketiga; (c) Mengurus sebarang perubahan terhadap pembekalan perkhidmatan dengan mengambil kira tahap kritikal perkhidmatan dan proses yang terlibat serta melaksanakan penilaian semula risiko keselamatan; dan (d) Pelan kontigensi perlu disediakan bagi memastikan kesediaan kemudahan pemprosesan maklumat bagi perkhidmatan kritikal yang disediakan oleh Pembekal dan Pihak Ketiga.	AGC, Pembekal dan Pihak Ketiga
0803 Perancangan dan Penerimaan Sistem Aplikasi **Objektif:** Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem aplikasi.	
080301 Perancangan Kapasiti	**Tanggungjawab**
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem aplikasi yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Kapasiti sesuatu komponen atau sistem aplikasi hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan, kegunaan dan operasi sistem aplikasi pada masa akan datang; dan (b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pemilik Sistem, ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
080302 Penerimaan Sistem Aplikasi	**Tanggungjawab**
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Semua sistem aplikasi baharu (termasuklah sistem aplikasi yang dikemas kini atau diubah suai) hendaklah memenuhi	Pemilik Sistem, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

<table>
<tr><td>kriteria yang ditetapkan dan juga mengikut garis panduan yang sedang berkuatkuasa sebelum diterima atau dipersetujui; dan

(b) Sistem aplikasi baharu hendaklah menjalani proses imbasan keselamatan dan melaksanakan tindakan pengukuhan sebelum digunakan.</td><td></td></tr>
<tr><td colspan="2">0804 Perisian Berbahaya
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, malware dan sebagainya.</td></tr>
<tr><td>080401 Perlindungan Dari Perisian Berbahaya</td><td>Tanggungjawab</td></tr>
<tr><td>Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran Pengguna terhadap serangan tersebut.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, IDS dan IPS serta memastikan prosedur penggunaan yang betul dan selamat diikuti;

(b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa;

(c) Mengimbas peralatan ICT dengan antivirus sebelum digunakan;

(d) Mengemas kini antivirus dengan paten antivirus yang terkini;

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

(f) Melaksanakan program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

(g) Memasukkan klausa tanggungan di dalam kontrak pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

(h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; dan

(i) Penggunaan MobileCode hendaklah daripada sumber yang dipercayai dan daripada perisian yang telah mendapat jaminan kualiti sahaja.</td><td>Pentadbir Sistem ICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT
AGC
dan Pengguna</td></tr>
<tr><td colspan="2"></td></tr>
</table>

0805 ***Housekeeping*** **Objektif:** Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
080501 ***Backup* dan *Restore***	**Tanggungjawab**
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di off site. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan *backup* keselamatan ke atas semua perisian aplikasi dan sistem aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Melaksanakan *backup* ke atas semua data dan maklumat mengikut keperluan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi; (c) Backup hendaklah dilakukan di dalam media yang bersesuaian; (d) Menguji secara berkala prosedur dan media backup dan restore bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan; (e) Membangun dan melaksana pengurusan generasi backup berdasarkan pelan pengurusan risiko bagi setiap aset ICT; (f) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat; dan (g) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan.	Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
0806 **Pengurusan Rangkaian** **Objektif:** Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
080601 **Kawalan Infrastruktur Rangkaian**	**Tanggungjawab**
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi sistem dan aplikasi dalam rangkaian daripada ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

(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 daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Peralatan keselamatan seperti firewall hendaklah dipasang bagi memastikan hak capaian ke atas sistem aplikasi dapat dilaksanakan; (e) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan; (f) Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran; (g) Memasang perisian IPS bagi mengesan sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem aplikasi dan maklumat AGC; dan (h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan AGC adalah tidak dibenarkan.	

0807 Pengurusan Media

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

080701 Pengurusan Media Boleh Alih	**Tanggungjawab**
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh AGC. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada Pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; (f) Media yang mengandungi maklumat terperingkat hendaklah dilupuskan mengikut prosedur yang telah ditetapkan; dan (g) Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Peralatan ICT terlebih dahulu.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir
080702 Pemindahan Media Fizikal	**Tanggungjawab**
Senarai syarikat kourier/pemindah yang diluluskan perlu diselenggara dan prosedur pengenalan syarikat kourier/ pemindah perlu diwujudkan. Log identiti bagi maklumat, masa pemindahan dan resit perlu diselenggara yang merupakan sebahagian dari prosedur tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pelupusan media fizikal perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan (b) Media fizikal yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan	Pegawai Aset dan Pentadbir Peralatan ICT

atau dimusnahkan mengikut prosedur yang berkuat kuasa.	
080703 Keselamatan Sistem Dokumentasi	**Tanggungjawab**
Sistem dokumentasi adalah merupakan komponen komunikasi, kawalan dan pemantauan dalam fasa pengurusan projek seperti pembangunan sistem, pengoperasian sistem dan penyelenggaraan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

0808 Keselamatan Pengkomputeran Awan

Objektif: Mengawal data dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang oleh penyedia perkhidmatan. Perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

080801 Pengurusan Pengkomputeran Awan	**Tanggungjawab**
Pengurusan pengkomputeran awan merupakan proses pemantauan dan memastikan keberkesanan dalam penggunaan pengkomputeran awam secara *public*, *private* atau *hybrid*. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan penyedia perkhidmatan memenuhi keselamatan siber, kerahsiaan dan kebolehpercayaan; (b) Menyediakan perjanjian perkhidmatan di antara AGC dengan penyedia perkhidmatan; (c) Memastikan SLA dilaksanakan (jika berkaitan); dan (d) Memastikan tiada kebocoran dan penyalahgunaan data.	PICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

0809 Perkhidmatan E-Dagang (Electronic Commerce Services)

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

080901 E-Dagang	**Tanggungjawab**
Proses menjalankan urusan perniagaan (membeli atau menjual	Pentadbir Sistem

barangan atau perkhidmatan) melalui rangkaian komputer atau internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (on-line) sama ada menggunakan private cloud, public cloud atau hybrid cloud perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; (c) Maklumat yang melibatkan transaksi dalam talian perlu dilindungi bagi mengelakkan transmisi yang tidak lengkap, mis-routing, pendedahan, pertindihan dan perubahan yang tidak dibenarkan; dan (d) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	ICT AGC dan Pengguna
0810 Pemantauan **Objektif:** Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
081001 Pengauditan dan Forensik ICT	**Tanggungjawab**
Pengauditan dan forensik ICT merupakan proses mengenal pasti bahan bukti fizikal dengan menggunakan teknologi dan sains forensik. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan jadual pelaksanaan disediakan; (b) Memastikan laporan dapatan dilaksanakan; (c) Memastikan tindakan pembetulan dilaksanakan; dan (d) Memastikan kemudahan penyimpanan log dan maklumat log dilindungi daripada pengubahan tidak sah dan capaian tanpa izin.	ICTSO, CSIRT AGC, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
081002 Jejak Audit	**Tanggungjawab**
Jejak audit sistem ICT adalah merupakan bukti yang didokumenkan dan adalah merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan maklumat jejak audit mengandungi identiti	Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (b) Jejak audit ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap akses yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan; (c) Jejak audit hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling semasa yang berkuatkuasa; dan (d) Jejak audit hendaklah dikawal bagi mengekalkan integriti data. Analisis ke atas jejak audit hendaklah dilakukan bagi mengesan: i. Kegagalan capaian; ii. Penggunaan yang tidak normal, contoh: akses terhadap sistem di luar waktu kebiasaan, kekerapan akses dan tempoh penggunaan yang berlainan dari kebiasaan; iii. Capaian ke atas rekod-rekod terhad; dan iv. Transaksi yang mencurigakan.	
081003 Sistem Log dan Pemantauan	**Tanggungjawab**
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem komputer ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/ pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (a) Fail log sistem pengoperasian; (b) Fail log servis (contoh: web, e-mel); (c) Fail log aplikasi (*audit trail*); dan (d) Fail log rangkaian (contoh: *switch, firewall*, IPS). Perkara-perkara yang perlu dipatuhi adalah seperti 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; (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, aktiviti ini hendaklah dilaporkan kepada ICTSO dan PICT; (d) Pemantauan berterusan boleh dibuat secara automatik dengan	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC

<table>
<tr><td>menggunakan perisian tertentu sebagai contoh pengimbas virus, algoritma check sum, password cracker, semakan integriti, pengesanan penceroboh dan analisis pemantauan prestasi sistem komputer; dan
(e) Teknologi yang digunakan untuk pemantauan berterusan boleh ditempatkan secara berpusat bagi menjalankan analisis terhadap log yang dikumpulkan dari pelbagai sistem.</td><td></td></tr>
<tr><td>081004 Penyeragaman Jam (Clock Synchronization)</td><td>Tanggungjawab</td></tr>
<tr><td>Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam AGC atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM).</td><td>Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC</td></tr>
<tr><td colspan="2">0811 Media Sosial
Objektif: Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.</td></tr>
<tr><td>081101 Keselamatan Media Sosial</td><td>Tanggungjawab</td></tr>
<tr><td>Keselamatan media sosial merupakan proses menyingkirkan ancaman keselamatan melalui pemantauan keselamatan siber.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara;
(b) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat;
(c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan;
(d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman;
(e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan;
(f) Tidak menyebarkan berita yang tidak sahih;
(g) Tidak melibatkan diri dengan aktiviti yang boleh menjurus kepada Cyber Stalking atau Cyber Harassment;
(h) Tidak menggunakan media sosial untuk tujuan peribadi semasa waktu pejabat sama ada menerusi peralatan komputer/peranti mudah alih yang dibekalkan oleh Kerajaan;
(i) Mematuhi dasar dan peraturan semasa berkaitan media sosial yang sedang berkuatkuasa; dan
(j) Memastikan keselamatan media sosial dengan melaporkan masalah yang berlaku seperti spam dan pencerobohan kepada penyedia perkhidmatan media sosial.</td><td>Pentadbir Media Sosial AGC</td></tr>
</table>

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 09:
KESELAMATAN KOMUNIKASI

BIDANG 09: KESELAMATAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian **Objektif:** Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
090101 Kawalan Rangkaian	**Tanggungjawab**
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman bagi AGC. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) Firewall hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (f) Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan MAMPU; (g) Semua trafik keluar dan masuk rangkaian di Pusat Data dan pejabat-pejabat cawangan hendaklah melalui firewall di bawah kawalan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (h) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer Pengguna; (i) Digalakkan memasang perisian bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat seperti berikut: i. IPS; ii. *Web Content Filtering*; dan iii. IDS. (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di AGC sahaja dan penggunaan rangkaian luar adalah dengan kelulusan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT; (l) Kemudahan bagi wireless LAN hendaklah dipantau dan dikawal penggunaannya;	PICT, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT dan Pentadbir Sistem ICT AGC

(m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (interface) yang bersesuaian di antara rangkaian AGC, rangkaian agensi lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; (p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan AGC; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap kawalan capaian AGC.	
090102 Keselamatan Perkhidmatan Rangkaian	**Tanggungjawab**
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse* atau *outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti. Mekanisme keselamatan dan tahap perkhidmatan hendaklah dimasukkan di dalam perjanjian perkhidmatan rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Komponen keselamatan rangkaian merangkumi perkakasan, perisian dan perkhidmatan perkomputeran awan digunakan bagi memastikan rangkaian selamat dari ancaman, serangan siber, cubaan pengodaman dan kecuaian Pengguna; (b) Sistem Keselamatan Rangkaian menggunakan kombinasi pelbagai komponen keselamatan rangkaian bagi membentuk sistem pertahanan berlapis/ *a layered defense system*; dan (c) Setiap lapisan sistem pertahanan membekal keupayaan pemantauan, pengenalan dan pemulihan bagi memastikan rangkaian selamat.	PICT, ICTSO, Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT, Pentadbir Sistem ICT AGC, Pembekal dan Pihak Ketiga
090103 Pengasingan Dalam Rangkaian	**Tanggungjawab**
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian AGC.	Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT dan Pentadbir

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti fungsi dan tanggungjawab pengguna; (b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Mengemaskinikan hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan (e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	Sistem ICT AGC
0902 Pemindahan/ Pertukaran Data dan Maklumat **Objektif:** Memastikan keselamatan perpindahan/ pertukaran data, maklumat dan perisian antara AGC dan pihak luar terjamin.	
090201 Polisi dan Prosedur Pemindahan/ Pertukaran Data dan Maklumat	**Tanggungjawab**
AGC perlu mengambil kira keselamatan maklumat apabila berlaku pemindahan data dan maklumat organisasi antara AGC dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Menyediakan perjanjian atau kebenaran bertulis untuk pertukaran maklumat dan perisian di antara AGC dengan pihak agensi luar; (c) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, didedahkan, disalah guna atau dirosakkan semasa pemindahan keluar dari AGC; dan (d) Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya.	PICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data Rangkaian dan Komunikasi ICT AGC dan Pengguna
090202 Perjanjian Mengenai Pemindahan/ Pertukaran Data dan Maklumat	**Tanggungjawab**
AGC perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan/pertukaran data dan maklumat organisasi antara AGC dengan pihak luar. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal penghantaran dan penerimaan maklumat;	CDO, Pemilik Sistem dan PICT AGC

(b) Memastikan prosedur keupayaan mengesan dan tanpa sangkalan semasa pemindahan/pertukaran data dan maklumat; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan/pertukaran data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	
090203 Pesanan Elektronik	**Tanggungjawab**
Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa yang sedang berkuatkuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan pesanan elektronik disediakan untuk memudahkan komunikasi antara Pengguna, Pembekal dan Pihak Ketiga hanya untuk kegunaan bisnes dengan sekatan-sekatan tertentu; (b) Penghantaran e-mel dan kepilan tidak berkaitan tugas rasmi harian adalah dilarang; (c) Mesej yang dihantar hendaklah ringkas dan ditujukan kepada yang berkenaan sahaja; (d) Mesej yang dihantar tidak menggunakan akaun orang lain melainkan dengan arahan yang telah ditetapkan; dan (e) Pengguna dilarang mengulang hantar/*forward* maklumat terhad tanpa kebenaran penghantar/ pemunya maklumat.	Pengguna
090204 Pengurusan E-mel	**Tanggungjawab**
E-mel merupakan surat, pesanan atau mesej dalam bentuk fail komputer yang dikirim dan diterima melalui sistem rangkaian komputer. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan akaun e-mel yang diperuntukkan oleh AGC sahaja sebagai e-mel rasmi; (b) Memastikan pengemaskinian peti e-mel (*mailbox*) dilaksanakan supaya kapasiti e-mel tidak melebihi kuota yang telah ditetapkan; (c) Menggunakan akaun e-mel rasmi untuk tujuan tugas rasmi sahaja; (d) Mengambil tindakan dan memberi maklum balas segera terhadap e-mel; dan (e) Memastikan e-mel rasmi yang dihantar atau diterima	Pengguna

disimpan mengikut prosedur pengurusan sistem fail elektronik yang telah ditetapkan.	
090205 Pengurusan Komunikasi Bersepadu (UC)	**Tanggungjawab**
Perkhidmatan komunikasi dan kolaborasi bersepadu yang diuruskan secara berpusat. Perkhidmatan ini menggabungkan saluran-saluran komunikasi e-mel, persidangan video dan audio, *instant messaging* serta Sistem Pengurusan Identiti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan setiap komunikasi yang dibuat untuk tujuan rasmi sahaja; (b) Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan; (c) Memastikan maklumat yang dihantar mengikut etika keselamatan yang ditetapkan; dan (d) Akaun yang diperuntukkan oleh AGC sahaja yang boleh digunakan.	Pengguna
090206 Perjanjian Kerahsiaan atau Ketakdedahan	**Tanggungjawab**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan AGC dan hendaklah disemak dan didokumentasikan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan Kerajaan yang sedang berkuatkuasa. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan; dan (b) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.	PICT, ICTSO, Pentadbir Sistem ICT AGC, Pembekal dan Pengguna

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 10:
PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

BIDANG 10: PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

1001 Keselamatan Dalam Membangunkan Sistem Aplikasi

Objektif: Memastikan sistem aplikasi yang dibangunkan sendiri atau Pembekal/ Pihak Ketiga mempunyai ciri-ciri keselamatan siber yang bersesuaian.

100101 Keperluan Keselamatan Sistem Aplikasi	**Tanggungjawab**
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem aplikasi baharu atau penambahbaikan pada sistem aplikasi sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambil kira kawalan keselamatan bagi memastikan tiada sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Mewujudkan dan melindungi persekitaran bagi pembangunan sistem aplikasi yang merangkumi keseluruhan kitar hayat pembangunan sistem aplikasi; (c) Ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi bagi memastikan integriti data dan sistem pemprosesan berjalan dengan betul dan sempurna; (d) Sistem aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; (e) Semua sistem aplikasi yang dibangunkan hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan; (f) memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; (g) Semua sistem aplikasi yang dibangunkan hendaklah menjalani sekurang-kurangnya UAT dan FAT; (h) Dokumentasi sistem aplikasi hendaklah disediakan bagi semua sistem aplikasi yang dibangunkan; dan (i) Semua sistem aplikasi yang hendak dibangunkan perlu mengikut keperluan pengguna dan selaras dengan garis panduan dan pekeliling semasa yang sedang berkuatkuasa.	Pemilik Sistem, Pembekal, Pihak Ketiga dan Pentadbir Sistem ICT AGC

100102 Pengesahan Data Input dan Output	Tanggungjawab
Data yang terlibat dalam sistem aplikasi perlu disahkan bagi memelihara integriti data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data input bagi sistem aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan tepat; (b) Data output daripada sistem aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; dan (c) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.	Pemilik Sistem, Pentadbir Sistem AGC, Pembekal dan Pihak Ketiga

1002 Keselamatan Fail Sistem Aplikasi

Objektif: Memastikan supaya fail sistem aplikasi dikawal dan dikendalikan dengan baik dan selamat.

100201 Kawalan Fail Sistem Aplikasi	Tanggungjawab
Fail sistem aplikasi perlu dikawal dan dikendalikan dengan baik dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT dan mengikut prosedur yang telah ditetapkan; (b) Kod sumber sistem aplikasi yang telah dikemaskini hanya boleh digunakan selepas diuji; (c) Mengawal capaian ke atas kod sumber sistem aplikasi bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, Pentadbir Sistem ICT, Pembekal dan Pihak Ketiga

1003 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif: Menjaga dan menjamin keselamatan sistem aplikasi.

100301 Prosedur Kawalan Perubahan	Tanggungjawab
Perubahan pada sistem aplikasi dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan Prosedur Kawalan Perubahan Sistem yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT

(a) Perubahan atau pengubahsuaian ke atas sistem aplikasi dan/atau pakej perisian hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Sistem aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian dan/atau pangkalan data untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan AGC. (c) PICT dan Pentadbir Sistem ICT perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh Pembekal; (d) Akses kepada kod sumber sistem aplikasi perlu dihadkan kepada Pengguna yang dibenarkan sahaja; dan (e) Sebarang kemungkinan kebocoran maklumat hendaklah dihalang.	
1004 Pembangunan Sistem Aplikasi **Objektif:** Memastikan supaya pembangunan sistem aplikasi secara *in-house* dan *outsource* diselia dan dipantau untuk memastikan ia mengikut jadual dan prosedur yang telah ditetapkan.	
100401 Prosedur Pembangunan Sistem Aplikasi	**Tanggungjawab**
Sistem aplikasi membantu Pengguna melaksanakan tugas rasmi harian. Contoh sistem aplikasi adalah sistem aplikasi pengurusan data. Sistem aplikasi juga merujuk kepada sistem aplikasi web dan sistem aplikasi mudah alih. Sistem aplikasi yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi berdasarkan Prosedur Pembangunan Sistem Aplikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Permohonan Pembangunan Sistem Aplikasi secara rasmi hendaklah dikemukakan kepada Urus Setia JPICT AGC untuk kelulusan; (b) Permohonan hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (c) Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di AGC bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; (d) Pembangunan sistem aplikasi mestilah menggunakan kod-kod piawaian di bawah DDSA dan sumber rujukan daripada Kementerian/Jabatan lain yang berkaitan; (e) Pemilik Sistem aplikasi bertanggungjawab mempromosi dan memastikan kelancaran pelaksanaan sistem; (f) Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; (g) Pemilik Sistem aplikasi perlu melaporkan kepada JPICT AGC secara berkala bagi kemajuan pelaksanaan sistem aplikasi; (h) Pembangunan sistem aplikasi hendaklah menggunakan	Pemilik Sistem dan Pentadbir Sistem ICT AGC

teknik pengaturcaraan dan pangkalan data yang selamat; (i) Sistem aplikasi AGC boleh didemonstrasi atau diagihkan kepada Kementerian/Jabatan lain dengan kebenaran PICT; (j) Kod sumber sistem aplikasi hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah direkodkan bagi tujuan kawalan versi; (k) Proses perolehan pembangunan sistem aplikasi secara outsource perlu dilakukan melalui prosedur perolehan yang sedang berkuatkuasa bagi mendapatkan perkhidmatan pembekal yang terbaik dan berwibawa; (l) Pembangunan sistem aplikasi secara *outsource* perlu diselia dan dipantau oleh Pemilik Sistem bagi memastikan kejayaan pelaksanaan projek; (m) Kod sumber (*source code*) bagi sistem aplikasi dan perisian adalah menjadi hak milik Kerajaan; (n) Kod sumber (*source code*) bagi sistem aplikasi yang dibangunkan perlu dilengkapi dengan penerangan terperinci; (o) *Transfer of Technology* (ToT) perlu dilaksanakan apabila pembangunan sistem aplikasi selesai atau berlaku pertukaran Pentadbir Sistem ICT; dan (p) Pembangunan sistem aplikasi yang melibatkan integrasi antara sistem hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	
1005 Kawalan Teknikal Keterdedahan (Vulnerability) **Objektif:** Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
100501 Kawalan Dari Ancaman Teknikal	**Tanggungjawab**
Kawalan daripada ancaman teknikal ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan maklumat ancaman diperolehi daripada sumber yang sahih; (b) Menilai tahap kerentanan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
100502 Kawalan Kod Sumber dan Dokumentasi Sistem Aplikasi	**Tanggungjawab**
Kawalan kod sumber dan dokumentasi sistem aplikasi hendaklah dilaksanakan ke atas sistem yang dibangunkan secara *outsource* dan *in-house.* Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan lancar sama ada selepas penyerahan sistem kepada Pemilik	Pentadbir Sistem ICT AGC

Sistem aplikasi atau pertukaran pegawai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan kod sumber dan dokumentasi bagi setiap sistem aplikasi yang dibangunkan disediakan sama ada secara *hardcopy* dan/atau *softcopy*; (b) Dokumentasi bagi konfigurasi integrasi antara sistem aplikasi disediakan; (c) Semua dokumentasi sistem aplikasi diletakkan secara berpusat, dikawal dan direkodkan; (d) Memastikan kod sumber sistem aplikasi dan dokumentasi menjadi hak milik Kerajaan; (e) Proses pengemaskinian fail sistem aplikasi hanya boleh dilakukan oleh Pentadbir Sistem ICT dan mengikut prosedur yang telah ditetapkan; (f) Sebarang pindaan ke atas fail atau kod sumber sistem aplikasi perlu dilaksanakan pengujian sebelum penggunaan; (g) Mengawal capaian ke atas kod sumber sistem aplikasi bagi mengelakkan pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan (h) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
100503 Kawalan Kod Selamat	**Tanggungjawab**
Persekitaran pembangunan yang selamat hendaklah dibina di atas infrastruktur IT yang boleh dipercayai dan selamat menggunakan perkakasan, perisian dan perkhidmatan serta pembekal yang selamat. Pengekodan selamat hendaklah termasuk: a) Penurunan kod dan pengeliruan; b) Mengelakkan jalan pintas; c) Pengimbasan automatik dan semakan kod; d) Mengelakkan komponen yang mempunyai kelemahan yang diketahui; dan e) Log dan Pengauditan.	Pentadbir Sistem ICT AGC
1006 Penamatan Sistem Aplikasi **Objektif:** Menerangkan prosedur yang perlu dilakukan apabila ingin menamatkan penggunaan sesuatu sistem aplikasi.	
100601 Penamatan Penggunaan Sistem Aplikasi	**Tanggungjawab**
Pemilik sistem aplikasi perlu memaklumkan penamatan penggunaan sistem aplikasi secara bertulis kepada Pegawai Aset AGC sekiranya tidak lagi digunakan/diperlukan.	Pemilik Sistem dan Pegawai Aset AGC

1007 Pembangunan Laman Web **Objektif:** Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan laman dan aplikasi web di AGC.	
100701 Prosedur Pengurusan Laman Web	**Tanggungjawab**
Laman Web adalah salah satu saluran penyebaran maklumat yang semakin penting antara kerajaan dan orang awam. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah mendapat kelulusan Jawatankuasa Pengurusan Laman Web; (b) Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab AGC; (c) Maklumat di laman web hendaklah dikemas kini dari semasa ke semasa; (d) Laman web agensi luar yang memerlukan pautan ke Laman Web AGC atau sebaliknya mestilah mendapat kebenaran Ketua Jabatan; dan (e) Pembangunan laman web hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam.	Pentadbir Sistem ICT AGC dan Pengguna
1008 Pembangunan Sistem Aplikasi Mudah Alih **Objektif:** Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan sistem aplikasi mudah alih.	
100801 Prosedur Pembangunan Sistem Aplikasi Mudah Alih	**Tanggungjawab**
Sistem aplikasi mudah alih yang selamat perlu dibangunkan meliputi seluruh kitar hayat pembangunan sistem aplikasi AGC. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pembangunan sistem aplikasi mudah alih hendaklah melaksanakan pengujian sebelum dimuatnaik; (b) Penyediaan langganan sistem aplikasi mudah alih kepada orang awam hendaklah melalui perkhidmatan GAMMA; dan (c) Pembangunan sistem aplikasi mudah alih yang melibatkan integrasi antara sistem hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	Pentadbir Sistem ICT AGC

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 11:
HUBUNGAN PEMBEKAL

BIDANG 11: HUBUNGAN PEMBEKAL

<table>
<tr><td colspan="2">1101 Keselamatan Maklumat Dalam Hubungan Pembekal
Objektif: Memastikan aset ICT AGC yang boleh dicapai/diakses oleh Pembekal dilindungi.</td></tr>
<tr><td>110101 Dasar Keselamatan Maklumat Untuk Hubungan Pembekal</td><td>Tanggungjawab</td></tr>
<tr><td>Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset AGC.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:
(a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;
(b) Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan Pembekal;
(c) Mengawal dan memantau akses oleh Pembekal;
(d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;
(e) Jenis-jenis obligasi kepada Pembekal;
(f) Pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;
(g) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber AGC kepada Pembekal;
(h) Menandatangani Surat Akuan Pematuhan PKS seperti LAMPIRAN 1; dan
(i) Pembekal perlu mematuhi Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.</td><td>Pemilik Sistem, PICT
dan
Pembekal</td></tr>
<tr><td>110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal</td><td>Tanggungjawab</td></tr>
<tr><td>Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap Pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat AGC. Pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak AGC selaras dengan peraturan dan kawalan keselamatan yang sedang berkuat kuasa.

Sekiranya Pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang Pembekal daripada melaksanakan perkhidmatan tersebut.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</td><td>Pembekal</td></tr>
</table>

(a) AGC hendaklah memilih pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; (b) Pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; (c) Semua wakil Pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; (d) Produk atau perkhidmatan yang ditawarkan oleh Pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (e) Penilaian teknikal oleh Jawatankuasa Penilaian Teknikal boleh dilaksanakan melalui laporan yang dikemukakan oleh Pembekal; (f) Laporan penilaian Pihak Ketiga yang dikemukakan oleh Pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: i. Badan penilai Pihak Ketiga adalah bebas dan berintegriti; ii. Badan penilai Pihak Ketiga adalah kompeten; iii. Kriteria penilaian; iv. Parameter pengujian; dan v. Andaian yang dibuat berkaitan dengan skop penilaian. (g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan AGC; dan (h) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh AGC.	
110103 Kawalan Keselamatan Maklumat Bagi Rantaian Bekalan ICT	**Tanggungjawab**
Perjanjian dengan pembekal utama hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan (c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pemilik Sistem, PICT dan Pembekal
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	

<table>
<tr><td colspan="2">Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian Pembekal</td></tr>
<tr><td>110201 Memantau dan Mengkaji Semula Perkhidmatan Pembekal</td><td>Tanggungjawab</td></tr>
<tr><td>AGC hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Memantau tahap prestasi perkhidmatan untuk mengesahkan Pembekal mematuhi perjanjian perkhidmatan;
(b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh Pembekal dan mengemukakan status kemajuan; dan
(c) Memaklumkan insiden keselamatan siber kepada pembekal oleh pemilik sistem seperti yang dikehendaki dalam perjanjian bagi penyelesaian insiden.</td><td>Pemilik Sistem, PICT
dan
Pembekal</td></tr>
<tr><td>110202 Menguruskan Perubahan Kepada Perkhidmatan Pembekal</td><td>Tanggungjawab</td></tr>
<tr><td>Perubahan kepada peruntukan perkhidmatan oleh Pembekal yang disebabkan oleh perubahan pada PKS AGC, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan data dan maklumat, sistem penyampaian dan proses perkhidmatan yang terlibat dan risiko.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

(a) Perubahan dalam perjanjian dengan Pembekal;
(b) Perubahan yang dilakukan oleh AGC bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
(c) Perubahan dalam perkhidmatan Pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran Pembekal dan subkontraktor.</td><td>Pemilik Sistem, PICT dan Pembekal</td></tr>
</table>

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 12:
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

BIDANG 12: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

1201 Mekanisme Pelaporan Insiden Keselamatan Siber

Objektif: Memastikan insiden keselamatan siber dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan siber.

120101 Mekanisme Pelaporan Insiden	Tanggungjawab
Insiden keselamatan siber hendaklah dilaporkan kepada ICTSO dengan kadar segera. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaporkan insiden keselamatan siber apabila: i. Maklumat disyaki/didapati hilang atau terdedah kepada pihak-pihak yang tidak diberi kuasa; ii. Sistem komputer disyaki atau digunakan tanpa kebenaran; iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; iv. Berlaku kejadian yang luar biasa kepada sistem komputer seperti kehilangan fail, sistem komputer kerap kali gagal dan komunikasi tersalah hantar; dan v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden keselamatan maklumat yang tidak dijangka. (b) Ringkasan bagi semua proses kerja yang terlibat dalam Pelaporan Insiden Keselamatan Siber di AGC seperti **LAMPIRAN 3**.	Pemilik Sistem, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC dan Pengguna

1202 Pengurusan Maklumat Insiden Keselamatan Siber

Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber.

120201 Prosedur Pengurusan Insiden Keselamatan Siber	Tanggungjawab
Sebarang insiden keselamatan siber hendaklah dikawal dengan menggunakan **Prosedur Pengurusan Insiden Keselamatan Siber** yang telah ditetapkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkaladan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat	ICTSO dan CERT AGC

aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan (sekiranya perlu); dan (d) Melapor kepada NACSA apabila berlaku sebarang insiden keselamatan siber (sekiranya perlu).	

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 13:
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BIDANG 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301 Dasar Kesinambungan Perkhidmatan

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

130101 Pelan Pengurusan Kesinambungan Perkhidmatan	Tanggungjawab
Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi memastikan kesinambungan perkhidmatan AGC. Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai pegawai AGC dan Pembekal berserta nombor yang boleh dihubungi (contoh: faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes, impak gangguan yang mungkin berlaku dan kesannya terhadap keselamatan siber serta tindakan bagi meminimumkan impak gangguan tersebut; (b) Melaksanakan prosedur tindak balas kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (e) Membuat backup mengikut keperluan DRP; (f) Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; (g) Pelan PKP hendaklah diuji sekurang-kurangnya setahun sekali	Koordinator PKP AGC, Pembekal dan Pengguna

atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; (h) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan PKP bersesuaian dan memenuhi tujuan dibangunkan; dan (i) Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 14:
PEMATUHAN

BIDANG 14: PEMATUHAN

1401 Pematuhan dan Keperluan Perundangan **Objektif:** Meningkatkan tahap keselamatan siber bagi mengelak daripada pelanggaran PKS AGC.	
140101 Pematuhan Dasar	**Tanggungjawab**
Pematuhan PKS AGC adalah diwajibkan kepada semua Pengguna, Pembekal dan Pihak Ketiga. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap Pengguna hendaklah membaca, memahami dan mematuhi PKS AGC serta undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa; (b) Semua aset ICT AGC termasuk data dan maklumat yang disimpan di dalamnya adalah hak milik Kerajaan; (c) ICTSO AGC berhak untuk memantau aktiviti Pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan; dan (d) Sebarang penggunaan aset ICT AGC selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber AGC.	Pengguna, Pembekal dan Pihak Ketiga
140102 Pematuhan Kepada Dasar, Piawaian dan Keperluan Teknikal	**Tanggungjawab**
Pematuhan kepada Dasar, Piawaian dan Keperluan Teknikal adalah pelengkap kepada pematuhan PKS AGC. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap Pengguna, Pembekal dan Pihak Ketiga perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal yang ditetapkan (jika ada); dan (b) Aset ICT perlu diperiksa dan dipantau secara berkala atau mengikut keperluan agar ia selaras dengan pematuhan dasar dan piawaian pelaksanaan keselamatan siber.	ICTSO, PICT AGC, Pembekal, Pihak Ketiga dan Pengguna
140102 Pematuhan Kepada Dasar, Piawaian dan Keperluan Teknikal	**Tanggungjawab**
Pematuhan kepada Dasar, Piawaian dan Keperluan Teknikal adalah pelengkap kepada pematuhan PKS AGC.	ICTSO, PICT AGC,

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap Pengguna, Pembekal dan Pihak Ketiga perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal yang ditetapkan (jika ada); dan (b) Aset ICT perlu diperiksa dan dipantau secara berkala atau mengikut keperluan agar ia selaras dengan pematuhan dasar dan piawaian pelaksanaan keselamatan siber.	Pembekal, Pihak Ketiga dan Pengguna
140103 Pematuhan Keperluan Audit	**Tanggungjawab**
Pematuhan terhadap keperluan audit bagi meminimumkan ancaman dan memaksimumkan keberkesanan aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas operasi aset ICT perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	ICTSO, PICT, Pentadbir Sistem ICT dan Pentadbir Pusat Data, Rangkaian dan Komunikasi ICT AGC
140104 Keperluan Perundangan	**Tanggungjawab**
Senarai perundangan dan peraturan yang perlu dipatuhi oleh pengguna aset ICT AGC adalah seperti **LAMPIRAN 4.** Pengguna, Pembekal dan Pihak Ketiga juga perlu mematuhi perundangan dan peraturan semasa yang sedang berkuat kuasa.	Pengguna, Pembekal dan Pihak Ketiga
140105 Pelanggaran Dasar	**Tanggungjawab**
Pelanggaran PKS AGC boleh diambil tindakan undang-undang dan/ atau tatatertib di bawah akta yang sedang berkuatkuasa.	Pengguna

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 15:
RISIKAN ANCAMAN (*THREAT INTELLIGENCE*)

BIDANG 15: RISIKAN ANCAMAN *(THREAT INTELLIGENCE)*

1501 Risikan Ancaman *(Threat Intelligence)*	
Objektif: Untuk memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.	
150101 Risikan Ancaman *(Threat Intelligence)*	**Tanggungjawab**
a) Risikan Ancaman ialah kerjasama dengan semua pasukan keselamatan maklumat dalam organisasi AGC; b) Perisian Risikan Ancaman boleh digunakan untuk pengumpulan risikan yang berkaitan bersama dengan kerjasama dengan semua pasukan keselamatan maklumat dalam organisasi; dan c) Sumber dalaman dan luaran boleh digunakan untuk pengumpulan risikan. Sumber tersebut mestilah relevan, tepat pada masanya dan boleh dipercayai.	Pengguna

JABATAN PEGUAM NEGARA (AGC)
JABATAN PERDANA MENTERI

BIDANG 16:
KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN *CLOUD*

BIDANG 16: KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN *CLOUD*

1601 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*

Objektif: Untuk menentukan dan mengurus keselamatan maklumat untuk penggunaan perkhidmatan *cloud*

160101 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan *Cloud*	**Tanggungjawab**
Peranan dan tanggungjawab dalam persekitaran *cloud* • Tanggungjawab dan peranan keselamatan maklumat yang dikongsi dalam penggunaan *cloud* di AGC harus diperuntukkan kepada pihak yang dikenal pasti, didokumenkan, dikomunikasikan dan dilaksanakan oleh kedua-dua pengguna dan pembekal perkhidmatan cloud. Mengalih keluar aset pelanggan perkhidmatan cloud • Aset pengguna perkhidmatan *cloud* yang berada di premis pembekal perkhidmatan *cloud* harus dialih keluar, dan dikembalikan, jika perlu, tepat pada masanya selepas penamatan terma dan syarat perkhidmatan di AGC. Keselamatan operasi pentadbir • Prosedur untuk operasi pentadbiran persekitaran pengkomputeran *cloud* harus ditakrifkan, didokumenkan dan dipantau. Pemantauan untuk Perkhidmatan *cloud* • Pengguna perkhidmatan *cloud* harus mempunyai keupayaan untuk memantau aspek tertentu operasi perkhidmatan *cloud* yang digunakan oleh pengguna perkhidmatan *cloud*. Pengasingan dalam persekitaran maya • Persekitaran maya pengguna perkhidmatan *cloud* yang berjalan pada pembekal perkhidmatan *cloud* harus dilindungi daripada pelanggan perkhidmatan cloud yang lain dan pihak yang tidak dibenarkan.	Pengguna dan Pembekal

11.0 Lampiran

11.0 LAMPIRAN

Berikut ialah lampiran-lampiran yang berkaitan sebagai panduan.

(i) Lampiran 1: Surat Akuan Pematuhan Polisi Keselamatan Siber AGC;

(ii) Lampiran 2: Proses Kerja Pelaporan Insiden Keselamatan Siber AGC; dan

(iii) Lampiran 3: Senarai Perundangan dan Peraturan.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER AGC

Nama (Huruf Besar) : ....

No. Kad Pengenalan : ....

Jawatan : ....

Bahagian (AGC)/Syarikat : ....

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber (PKS) 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

....

(Tandatangan dan Nama ICTSO)

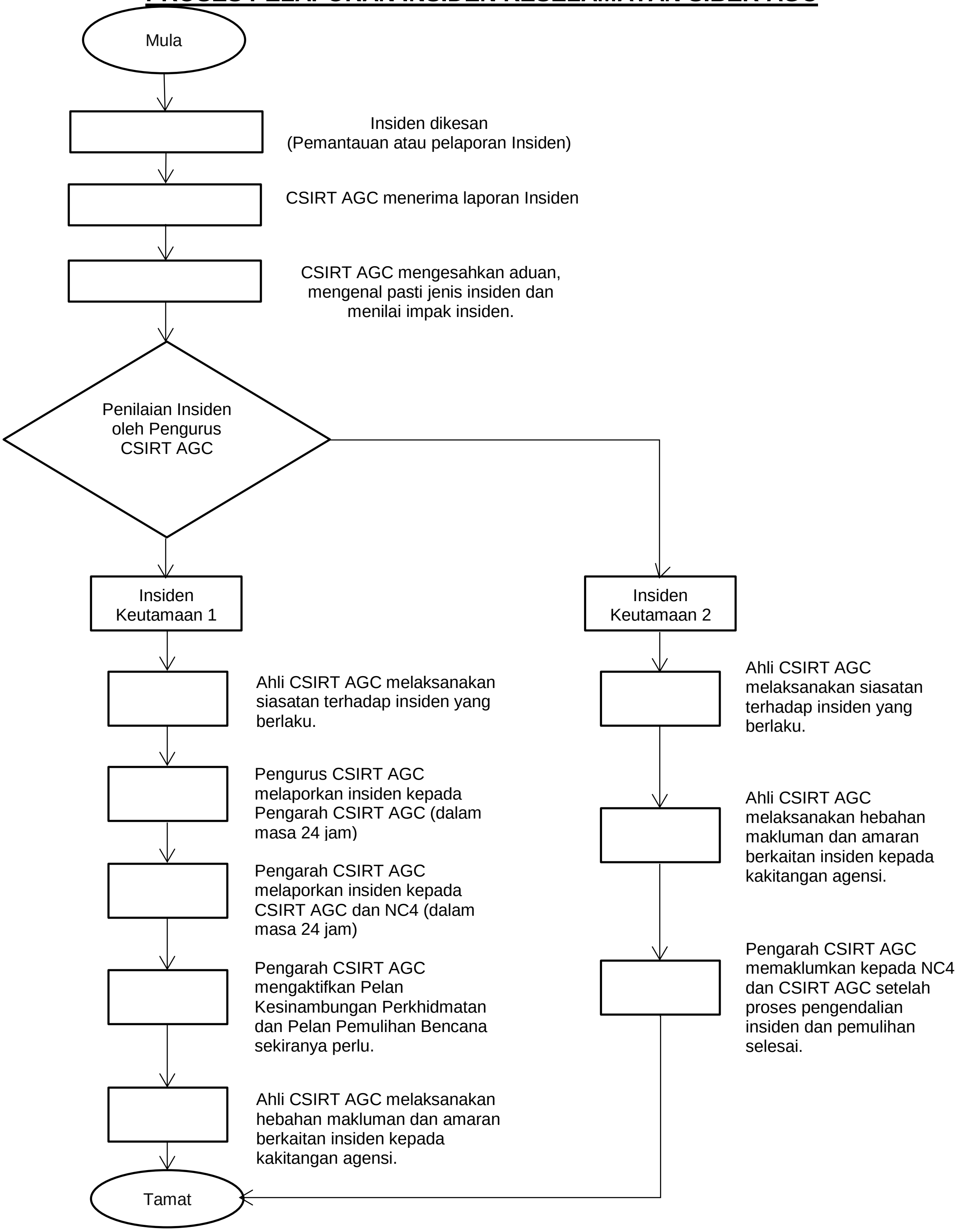
b.p Peguam Negara

Tarikh: ....

Cap rasmi Jawatan:

LAMPIRAN 2

PROSES PELAPORAN INSIDEN KESELAMATAN SIBER AGC



LAMPIRAN 3

SENARAI PERUNDANGAN DAN PERATURAN

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
1.	Akta 88 - Akta Rahsia Rasmi 1972.	SPRM
2.	Akta 332 – Akta Hak Cipta Tahun 1987.	KPDNKK (Perbadanan Harta Intelek Malaysia)
3.	Akta 563 - Akta Jenayah Komputer 1997 bertarikh 30 Jun 1997.	Jabatan Peguam Negara
4.	Akta 588 - Akta Komunikasi dan Multimedia 1998 bertarikh 15 Oktober 1998.	SKMM
5.	Akta 589 - Akta Suruhanjaya Komunikasi dan Multimedia 1998 bertarikh 15 Oktober 1998.	SKMM
6.	Akta 562 - Akta Tandatangan Digital 1997 bertarikh 30 Jun 1997.	Jabatan Peguam Negara
7.	Akta 680 - Akta Aktiviti Kerajaan Elektronik 2007.	MAMPU
8.	Akta 629 - Akta Arkib Negara 2003.	Kementerian Pelancongan dan Kebudayaan Malaysia (Arkib Negara Malaysia)
9.	Akta 709 - Akta Perlindungan Data Peribadi 2010.	Kementerian Komunikasi dan Multimedia Malaysia (Jabatan Perlindungan Data Peribadi)
10.	Arahan Perbendaharaan Malaysia 150(i) bertarikh 31 Julai 2008.	Kementerian Kewangan Malaysia
11.	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000.	MAMPU
12.	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) bertarikh 4 April 2001.	MAMPU
13.	Pekeliling Am Bilangan 2 Tahun 2002 - Penggunaan dan Pemakaian Data *Dictionary* Sektor Awam (DDSA) Sebagai *Standard* di Agensi- Agensi Kerajaan bertarikh 2 September 2002.	MAMPU
14.	Pekeliling Am Bilangan 2 Tahun 2006 - Pengukuhan Tadbir Urus Jawatankuasa IT dan Internet Kerajaan bertarikh 13 November 2006.	MAMPU
15.	Pekeliling Am Bil. 1 Tahun 2009 - Manual Pengurusan Aset Menyeluruh Kerajaan bertarikh 27 Mac 2009.	JPM
16.	Pekeliling Am Bilangan 3 Tahun 2011 - Pemansuhan Keperluan Mengemukakan Laporan Polis Yang Tidak Merupakan Suatu Kehendak Undang-Undang dalam Berurusan Dengan Agensi Kerajaan	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	bertarikh 29 September 2011.	
17.	Pekeliling Am Bilangan 1 Tahun 2012 - Pemansuhan Keperluan Pengesahan Yang Tiada Nilai Tambah pada Borang Rasmi Kerajaan dan Salinan Dokumen Sokongan bertarikh 2 Mac 2012.	MAMPU
18.	Pekeliling Am Bilangan 2 Tahun 2012 - Tatacara Pengurusan Aset Tak Alih Kerajaan bertarikh 21 Jun 2012.	JPM
19.	Pekeliling Am Bilangan 3 Tahun 2012 - Sistem Kod Aset Tak Alih bertarikh 21 Jun 2012.	JPM
20.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam bertarikh 30 September 2015.	MAMPU
21.	1 Pekeliling Perbendaharaan (1PP).	Kementerian Kewangan Malaysia
22.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 - Panduan Pengurusan Pejabat bertarikh 30 April 2007.	JPA
23.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan bertarikh 28 November 2003.	MAMPU
24.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 - Pengurusan Laman Web Agensi Sektor Awam bertarikh 30 September 2015.	MAMPU
25.	Pekeliling Transformasi Pentadbiran Awam Bil.1 Tahun 2017 – Pelaksanaan Analitis Data Raya Sektor Awam (aDRSA).	MAMPU
26.	Pekeliling Transformasi Pentadbiran Awam Bil. 3 Tahun 2017 – Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (*Government Unified Communication* (1GovUC))	MAMPU
27.	Surat Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2019 – Penyeragaman Lokasi Dan Reka Bentuk Pautan Borang Aduan Dan Maklum Balas Dalam Laman Web Agensi Sektor Awam.	MAMPU
28.	Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2020 – MyGovEA: Pelaksanaan Pendekatan Reka Bentuk Berstruktur Ekosistem Organisasi Perkhidmatan Awam.	MAMPU
29.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021– Dasar Perkhidmatan Pengkomputeran Awam Sektor Awam.	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
30.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2021- Dasar Perkongsian Data Sektor Awam.	MAMPU
31.	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.	JPM
32.	Surat Arahan Ketua Setiausaha Negara - Langkah- Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran atau Kuasa yang Sah di Agensi-agensi Kerajaan bertarikh 31 Januari 2007.	JPM
33.	*Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002 bertarikh 15 Januari 2002	MAMPU
34.	Arahan Teknologi Maklumat 2007 bertarikh 19 Disember 2007.	MAMPU
35.	Arahan Keselamatan Kerajaan (Semakan dan Pindaan 2017).	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
36.	Surat Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 - Pematuhan Tatacara Penggunaan E-mel dan Internet	MKN
37.	Surat Arahan Ketua Pengarah MAMPU - Langkah- Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007.	MAMPU
38.	Surat Arahan Ketua Pengarah MAMPU - Langkah- Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.	MAMPU
39.	Surat Arahan Ketua Pengarah MAMPU - Pengaktifan Fail Log Server bertarikh 23 Mac 2009.	MAMPU
40.	Surat Arahan Ketua Pengarah MAMPU – Panduan Penyediaan dan Penyiaran Berita *Online* di Laman Web Agensi-agensi Kerajaan bertarikh 11 September 2009.	MAMPU
41.	Surat Arahan Ketua Pengarah MAMPU - Penggunaan *Smartphone*, *Personal Digital Assistant* dan Alat Komunikasi	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	Mudah Alih Sebagai Saluran Komunikasi Tambahan bertarikh 15 September 2009.	
42.	Surat Arahan Ketua Pengarah MAMPU - Penggunaan Media Sosial di Sektor Awam bertarikh 19 November 2009.	MAMPU
43.	Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi IPv6 Sektor Awam yang bertarikh 4 Januari 2010.	MAMPU
44.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	MAMPU
45.	Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam yang bertarikh 5 Mac 2010.	MAMPU
46.	Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan dan Pengurusan E-Mel di Agensi-Agensi Kerajaan yang bertarikh 1 Julai 2010.	MAMPU
47.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam yang bertarikh 24 November 2010.	MAMPU
48.	Surat Arahan Ketua Pengarah MAMPU - Amalan Terbaik Penggunaan Media Jaringan Sosial di Sektor Awam bertarikh 8 April 2011.	MAMPU
49.	Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan dan Penggunaan Aplikasi *Digital Document Management System* (DDMS) Sektor Awam bertarikh 26 Januari 2015.	MAMPU
50.	Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Rasionalisasi Laman Web bertarikh 26 Mei 2015.	MAMPU
51.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App. 2.0 Di Agensi Sektor Awam bertarikh 12 Ogos 2015.	MAMPU
52.	Surat Arahan Ketua Pengarah MAMPU Bilangan 1 Tahun 2021 – Garis Panduan Perkhidmatan Galeri Aplikasi Mudah Alih Kerajaan Malaysia (GAMMA)	MAMPU
53.	Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK) bertarikh 20 Disember 2000.	MAMPU
54.	Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
	Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.	
55.	Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam bertarikh 9 November 2006.	MAMPU
56.	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009.	MAMPU
57.	Surat Pekeliling Am Bilangan 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan	MAMPU
58.	Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003	MAMPU
59.	Garis Panduan *IT Outsourcing* 2006 bertarikh Oktober 2006.	MAMPU
60.	Garis Panduan Penggunaan ICT ke arah ICT Hijau dalam Perkhidmatan Awam 2010 bertarikh 3 Ogos 2010.	MAMPU
61.	Garis Panduan Pengurusan Projek Sektor Awam (PPriSA).	MAMPU
62.	Garis Panduan Pembangunan Aplikasi/ Kejuruteraan Sistem aplikasi Sektor Awam (KRISA).	MAMPU
63.	Risalah Penerapan Etika Penggunaan Media Sosial dalam Sektor Awam – Mac 2015.	MAMPU
64.	Surat Pemberitahuan Mengenai Penyerahan Fungsi Keselamatan Siber Dan Dasar/ Pekeliling/ Penerbitan Berkaitan Keselamatan ICT Kerajaan Kepada Agensi Keselamatan Siber Negara rujukan MAMPU.700-5/12/1 Jld 3 (35) bertarikh 17 September 2021.	MAMPU / NACSA