POLISI KESELAMATAN SIBER

VERSI 1.0

BERSEKUTU BERTAMBAH MUTU

BAHAGIAN HAL EHWAL UNDANG-UNDANG
JABATAN INSOLVENSI MALAYSIA
JABATAN BANTUAN GUAMAN

SEJARAH DOKUMEN

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	Mesyuarat JPICT BHEUU Bil. 2/2022	3 Jun 2022

KANDUNGAN

TAKRIFAN

1.	Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
2.	Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
4.	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
5.	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6.	*Bandwidth*	Jalur lebar. Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
7.	BCP/PKP	*Business Continuity Planning*/Pengurusan Kesinambungan Perkhidmatan

8.	BHEUU	Bahagian Hal Ehwal Undang-Undang termasuk Pejabat YB Menteri (Undang-Undang dan Parlimen) dan Pejabat YB Timbalan Menteri (Undang-Undang dan Parlimen).
9.	CCTV	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
10.	CERT BHEUU	*Computer Emergency Response Team* (CERT) atau Pasukan Tindakan Kecemasan BHEUU.
11.	CIA	*Confidentiality, Integrity and Availability.*
12.	CGSO	*Chief Government Security Officer.* Ketua Pegawai Keselamatan Kerajaan.
13.	CIO	*Chief Information Officer.* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
14.	*Clear Desk* dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.

15.	*Data-at-rest* (data-dalam-simpanan)	*Refers to data that is being stored in stable destination system. Data at rest is frequently defined as data that is not in use or is not traveling to system endpoints, such as mobile devices or workstations.*
16.	*Data-in-motion* (data-dalam-pergerakan)	*Refers to a stream of data moving through any kind of network. It represents data which is being transferred or moved.*
17.	*Data-in-use* (data-dalam-penggunaan)	*Refers to data that is not simply being passively stored in a stable destination, such as a central data warehouse, but is working its way through other parts of an IT architecture.*
18.	*Denial of service*	Halangan pemberian perkhidmatan.
19.	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu makenisme lapisan pertahanan untuk melindungi data dan maklumat.
20.	*Downloading*	Aktiviti muat turun sesuatu perisian.
21.	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
22.	*Firewall*	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam

		bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
23.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
24.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
25.	*Hub*	*Hub* merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu *port* kepada semua *port* yang lain.
26.	ICT	*Information and Communication Technology.* Teknologi Maklumat dan Komunikasi.
27.	ICTSO	*ICT Security Officer* (Pegawai Keselamatan ICT). Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
28.	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.

29.	Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
30.	Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
31.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
32.	*Internet Gateway*	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
33.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
34.	*Intrusion Detection System* (IDS)	Sistem Pengesan Pencerobohan. Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.

35.	*Intrusion Prevention System* (IPS)	Sistem Pencegah Pencerobohan. 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 atau *malicious code*. Contoh: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
36.	ISDN	*Integrated Services Digital Networks.* Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
37.	Jabatan	Bahagian Hal Ehwal Undang-Undang (BHEUU), Jabatan Insolvensi Malaysia (MdI) dan Jabatan Bantuan Guaman (JBG).
38.	JBG	Jabatan Bantuan Guaman.
39.	JPICT	Jawatankuasa Pemandu ICT.
40.	Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
41.	Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran Keselamatan.

42.	Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
43.	LAN	*Local Area Network.* Rangkaian Kawasan Setempat yang menghubungkan komputer.
44.	*Lock*	Mengunci komputer.
45.	*Logout*	Log keluar daripada sistem komputer. Keluar daripada sesuatu sistem atau aplikasi komputer.
46.	*Malicious Code*	Kod hasad. Perkakasan atau perisian yang telah dimasukan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
47.	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia.
48.	MdI	Jabatan Insolvensi Malaysia.
49.	*Mobile Code*	*Mobile code* merupakan suatu perisian yang boleh dipindahkan di antara komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses

		pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
50.	*MODEM*	*MOdulator DEModulator.* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
51.	*Outsource*	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
52.	Pegawai Pengelas	Pegawai yang bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
53.	Pembekal	Pembekal adalah syarikat yang dilantik Kerajaan untuk membekalkan barangan atau perkhidmatan ICT kepada Jabatan.
54.	Pengarah Seksyen	Merujuk kepada Pengarah Seksyen/Bahagian/Ketua Unit Jabatan.

55.	Pengguna	Merujuk warga Jabatan, pembekal dan pihak-pihak lain yang diberi kebenaran menggunakan perkhidmatan ICT.
56.	Pengolahan Risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
57.	Pengurusan Sumber Manusia	Merujuk kepada Seksyen Pengurusan Sumber Manusia BHEUU, Bahagian Khidmat Pengurusan MdI dan Unit Sumber Manusia JBG.
58.	Pentadbir Media Sosial	Merujuk kepada Unit Komunikasi Korporat BHEUU, Bahagian Dasar, Perundangan dan Komunikasi Strategik MdI dan Pegawai Perhubungan Awam JBG
59.	Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
60.	*Public-Key Infrastructure (PKI)*	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
61.	*Rollback* (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.

62.	*Router*	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contoh, pencapaian Internet.
63.	Ruang Siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
64.	*Screen saver*	Imej yang akan diaktifkan pada sistem/komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
65.	*Server*	Pelayan komputer.
66.	SIRIM	Standard and Industrial Research Institute of Malaysia. Institut Piawaian dan Penyelidikan Perindustrian Malaysia.
67.	*Source Code*	Kod sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.

68.	*Switch*	*Switch* merupakan gabungan *hub* dan *bridge* untuk melaksanakan *screen filtering* supaya dapat mensegmenkan rangkaian. Kegunaan *switch* dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/ Collision Detection* (CSMA/CD) yang merupakan satu sistem penghantaran dengan mengurangkan pelanggaran yang berlaku.
69.	*Threat*	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
70.	*Uninterruptible Power Supply* (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
71.	*Video Conference*	Persidangan video. Persidangan/mesyuarat/perbincangan secara maya di mana peserta yang berada di lokasi berbeza boleh berkomunikasi sesama sendiri melalui audio dan video.
72.	*Video Streaming*	Teknologi menghantar fail audio dan video secara berterusan melalui internet.
73.	*Virus*	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.

74.	*WAN*	*Wide Area Network.* Rangkaian yang merangkumi kawasan yang luas.
75.	Warga Jabatan	Kakitangan Kerajaan yang berkhidmat di BHEUU, MdI dan JBG sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT Jabatan.
76.	*Wireless LAN*	Jaringan komputer yang terhubung tanpa melalui kabel.

TUJUAN

1. Polisi Keselamatan Siber BHEUU, MdI dan JBG ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan dalam melindungi aset ICT Jabatan.

LATAR BELAKANG

2. Polisi ini dibangunkan untuk menjamin kesinambungan urusan Jabatan dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi Jabatan bagi memastikan semua aset ICT dilindungi.

OBJEKTIF

3. Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti berikut:

   i. Menerangkan kepada semua pengguna merangkumi warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT;

   ii. Memastikan keselamatan penyampaian perkhidmatan Jabatan di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

iii. Memastikan kelancaran operasi Jabatan dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

iv. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

v. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

ASET ICT

4. Aset ICT Jabatan merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut:

i. Maklumat

Semua penyedia perkhidmatan dalam Jabatan hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

a. Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuk apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang

berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

b. Maklumat Rasmi

Maklumat rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh Jabatan semasa menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

c. Maklumat Pengenalan Peribadi (Personally Identifiable Information (PII))

Maklumat Pengenalan Peribadi (Personally Identifiable Information (PII)) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

d. Data Terbuka

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. PII dikecualikan daripada data terbuka.

ii. Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi.

Aliran data dan komunikasi dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

a. Saluran komunikasi dan aliran data antara sistem di Jabatan;

b. Saluran komunikasi dan aliran data ke sistem luar; dan

c. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

iii. Platform Aplikasi dan Perisian

Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

iv. Peranti Fizikal dan Sistem

Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

a. Pelayan;

b. Peranti/ Peralatan Rangkaian;

c. Komputer Peribadi/ Komputer Riba;

d. Telefon/ Peranti Pintar;

e. Media Storan;

f. Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);

g. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan

h. Peranti pengesahan (authentication devices), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

v. Sistem Luaran

Sistem luaran ialah sistem bukan milik Jabatan yang dihubungkan dengan sistem Jabatan. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

vi. Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Jabatan. Contoh perkhidmatan sumber luaran ialah:

a. Perisian Sebagai Satu Perkhidmatan (Software as a Service atau SaaS);

b. Platform Sebagai Satu Perkhidmatan (Platform as a Service atau PaaS);

c. Infrastruktur Sebagai Satu Perkhidmatan (Infrastructure as a Service atau IaaS);

d. Storan Pengkomputeran Awan; dan

e. Pemantauan Keselamatan.

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

PENILAIAN RISIKO KESELAMATAN ICT

5. Jabatan hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian Jabatan tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber Jabatan.

6. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran ruang siber Jabatan.

7. Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

i. Kerentanan (Vulnerability)

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

ii. Ancaman

Jabatan hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

iii. Impak

Jabatan hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi Jabatan.

iv. Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

v. Penguraian Risiko

a. Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/ faedahnya.

b. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

1) Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, *firewall* digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

2) Proses

Rekayasa semula (re-engineering) proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3) Manusia

Mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

vi. Pengurusan Risiko

Penyedia perkhidmatan digital di Jabatan hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

a. Mengenal pasti kerentanan;

b. Mengenal pasti ancaman;

c. Menilai risiko;

d. Menentukan penguraian risiko;

e. Memantau keberkesanan penguraian risiko; dan

f. Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

PRINSIP KESELAMATAN

8. Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, Jabatan hendaklah melaksanakan prinsip keselamatan seperti yang berikut:

i. Prinsip “Perlu-Tahu”

Jabatan hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja. Bagi capaian spesifik maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi, peranan dan fungsi pengguna tersebut.

ii. Hak Keistimewaan Minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap 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. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/ bidang tugas.

iii. Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (check and balance), Jabatan hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

iv. Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

v. Peminimuman Data

Jabatan hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

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

i. Peringkat Pemprosesan Data

a. Data-dalam-simpanan

1) Jabatan 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.

2) Maklumat Rahsia Rasmi, Maklumat Rasmi dan Maklumat Pengenalan Peribadi (PII) perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

b. Data-dalam-pergerakan

Jabatan 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.

c. Data-dalam-penggunaan

1) Jabatan 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.

2) Teknologi yang bersesuaian boleh digunakan oleh Jabatan untuk memastikan asal data dan data/ transaksi tanpa-sangkal.

d. Perlindungan Ketirisan Data

1) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

2) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

ii. Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, Jabatan hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (counter and 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 Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan seperti di bawah:

a. Peranti Pengkomputeran Peribadi

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

2) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada Jabatan. 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 pengolahan risiko.

b. Peranti Rangkaian

1) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, *router*, *firewall*, *Virtual Private Network* (VPN) dan kabel.

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-pergerakan dan bagi menghalang ketirisan data.

c. Aplikasi

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

d. Pelayan

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

2) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

e. Persekitaran Fizikal

1) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

2) Jabatan 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.

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

4) Teknologi dan kawalan keselamatan perlu dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan dan data-dalam-simpanan bagi menghalang ketirisan data.

f. Pengkomputeran Awan

1) Pengkomputeran awan merujuk lokasi yang menempatkan sistem ICT menggunakan perkhidmatan pengkomputeran awan yang disediakan melalui internet oleh pihak ketiga dikenali sebagai Penyedia Perkhidmatan Awan (Cloud Service Provider (CSP)).

2) MAMPU dalam persekitaran yang terkawal, selamat, berasaskan standard dan amalan terbaik global telah menyediakan perkhidmatan pengkomputeran awan di Pusat Data Sektor Awam (PDSA) kepada Agensi Sektor Awam yang dikenali sebagai perkhidmatan MyGovCloud@PDSA.

3) Pelaksanaan projek ICT hendaklah menggunakan pengkomputeran awan dengan memberikan keutamaan kepada penggunaan perkhidmatan MyGovCloud@PDSA terutamanya yang melibatkan aplikasi kritikal kerajaan.

4) Jabatan hendaklah merujuk kepada MAMPU untuk mendapatkan nasihat mengenai perkhidmatan pengkomputeran awan yang akan dilaksanakan dan mematuhi polisi yang digariskan.

PROSES

10. Jabatan hendaklah melindungi keselamatan ICT dengan melaksanakan perkara-perkara berikut:

i. Konfigurasi Asas

a. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan.

b. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

ii. Kawalan Perubahan Konfigurasi

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

b. 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.

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

iii. Sandaran dan Pemulihan (Backup and Restore)

a. Sandaran dan pemulihan hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa untuk memastikan bahawa proses kerja boleh dilaksanakan.

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

iv. Kitaran Pengurusan Aset

a. Pindah

1) Pemindahan hak milik aset berlaku dalam keadaan berikut:

i) Warga Jabatan meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

ii) Aset yang dikongsi untuk kegunaan sementara;

iii) Pemberian aset kepada agensi lain; dan

iv) Aset dikembalikan setelah tamat tempoh sewaan.

2) Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (b).

b. Pelupusan

1) 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.

2) 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 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

3) Pelupusan boleh dalam bentuk pemusnahan fizikal dan/ atau sanitasi data.

4) Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

c. Kitaran Hayat

1) Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

2) Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

11. Warga Jabatan, pembekal dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

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

    i. Kompetensi Pengguna

        a. Kompetensi pengguna termasuk:

            1) Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan ICT dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan ICT.

            2) Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga Jabatan berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

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

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

ii. Kompetensi Pelaksana

a. Warga Jabatan yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

b. ICTSO hendaklah memenuhi syarat-syarat berikut:

1) Mempunyai pengetahuan asas dalam keselamatan ICT;

2) Mempunyai pengalaman dalam bidang keselamatan ICT; dan

3) Telah menjalani tapisan keselamatan daripada agensi yang diberi kuasa.

c. ICTSO yang dilantik oleh Jabatan hendaklah memenuhi keperluan kompetensi di atas. ICTSO bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan ICT di Jabatan.

iii. Peranan Pengguna

a. Peranan pengguna hendaklah diberi berdasarkan keperluan dan bidang tugas pengguna.

b. Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan.

Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

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

d. Warga Jabatan yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.

e. Warga Jabatan yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

f. Warga Jabatan lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan.

PERNYATAAN POLISI KESELAMATAN SIBER

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

14. Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara

keselamatan aset ICT dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

i. Kerahsiaan

Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

ii. Integriti

Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

iii. Tidak Boleh Disangkal
Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

iv. Kesahihan

Data dan maklumat hendaklah dipastikan kesahihannya.

v. Ketersediaan

Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

15. Selain itu, langkah-langkah ke arah memelihara keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT Jabatan, ancaman yang wujud akibat daripada

kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

16. Sebanyak 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber BHEUU, MdI dan JBG diterangkan dengan lebih jelas dan teratur seperti berikut:

PERKARA	PERANAN
BIDANG 01 : POLISI KESELAMATAN MAKLUMAT	
1.1 HALA TUJU PENGURUSAN UNTUK KESELAMATAN MAKLUMAT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Jabatan dan perundangan yang berkaitan.	
1.1.1 POLISI KESELAMATAN MAKLUMAT	
Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah BHEUU dengan disokong oleh JPICT yang terdiri daripada CIO, ICTSO, Pengarah Seksyen dan ahli-ahli yang dilantik oleh Ketua Pengarah BHEUU. Polisi Keselamatan Siber mestilah dipatuhi oleh semua warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan BHEUU kepada warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan.	Ketua Pengarah BHEUU/CIO/ ICTSO/Pengarah Seksyen/JPICT
1.1.2 KAJIAN SEMULA POLISI UNTUK KESELAMATAN MAKLUMAT	
Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi Kerajaan. Berikut ialah prosedur	CIO/ICTSO/ JPICT

PERKARA	PERANAN
yang berkaitan dengan kajian semula Polisi Keselamatan Siber BHEUU, MdI dan JBG: i. Mengenal pasti dan menentukan perubahan yang diperlukan; ii. Mengemukakan cadangan pindaan untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan; iii. Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan; dan iv. Polisi ini hendaklah dikaji semula setiap **LIMA (5) TAHUN SEKALI** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	
BIDANG 02 : PERANCANGAN BAGI KESELAMATAN ORGANISASI	
2.1 PERANCANGAN DALAMAN	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber BHEUU, MdI dan JBG.	
2.1.1 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT	
i. Memastikan penguatkuasaan pelaksanaan Polisi ini;	Ketua Pengarah BHEUU

PERKARA	PERANAN
ii. Memastikan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; iii. Memastikan semua keperluan Jabatan seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; iv. Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ini; v. Melantik CIO dan ICTSO; dan vi. Mempengerusikan Mesyuarat JPICT.	
CIO bagi BHEUU, MdI dan JBG adalah terdiri daripada: **Jabatan** / **CIO** BHEUU — Timbalan Ketua Pengarah (Pengurusan) MdI — Timbalan Ketua Pengarah (Pengurusan) JBG — Timbalan Ketua Pengarah (Sivil) Peranan dan tanggungjawab Timbalan Ketua Pengarah (Pengurusan) BHEUU sebagai CIO adalah seperti berikut: i. Mewujud dan mengetuai pasukan penyelaras keselamatan ICT Jabatan;	CIO

<table>
<tr><th>PERKARA</th><th>PERANAN</th></tr>
<tr><td>
ii. Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT seperti yang ditetapkan di dalam Polisi ini;

iii. Memastikan kawalan keselamatan ICT dalam Jabatan diseragam dan diselaraskan dengan sebaiknya;

iv. Memastikan Pelan Strategik ICT Jabatan mengandungi aspek keselamatan ICT; dan

v. Memantau pembangunan dan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT; dan

vi. Mempengerusikan Mesyuarat Jawatankuasa ICT (JTICT).
</td><td></td></tr>
<tr><td>
ICTSO bagi BHEUU, MdI dan JBG adalah terdiri daripada:

<table>
<tr><th>Jabatan</th><th>ICTSO</th></tr>
<tr><td>BHEUU</td><td>Pengarah Seksyen Pengurusan Maklumat</td></tr>
<tr><td>MdI</td><td>Pengarah Bahagian Teknologi Maklumat</td></tr>
<tr><td>JBG</td><td>Pegawai Teknologi Maklumat</td></tr>
</table>

Peranan dan tanggungjawab Pengarah Seksyen Pengurusan Maklumat BHEUU sebagai ICTSO adalah seperti berikut:
</td><td>ICTSO</td></tr>
</table>

PERKARA	PERANAN
i. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; ii. Mengenal pasti punca ancaman atau insiden keselamatan ICT, memperakui dan menyelaras pelaksanaan langkah-langkah kawalan keselamatan ICT berpandukan rangka kerja, polisi dan pekeliling/garis panduan yang berkuat kuasa; iii. Melaporkan insiden keselamatan ICT kepada CERT BHEUU dan seterusnya menyelaras penyiasatan atau pemulihan insiden berkaitan; iv. Melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan PKP; v. Melaksanakan pematuhan Polisi ini oleh warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan; dan vi. Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT.	
Pengurus Keselamatan ICT ialah Ketua Penolong Pengarah (Operasi) Seksyen Pengurusan Maklumat. Peranan dan tanggungjawab Pengurus Keselamatan ICT adalah seperti berikut:	Pengurus Keselamatan ICT

PERKARA	PERANAN
i. Mengkaji dan menetapkan kawalan keselamatan ICT agar ianya berselaras dengan keperluan Jabatan; ii. Menentukan kawalan capaian semua pengguna terhadap aset ICT; iii. Melaporkan ancaman atau insiden keselamatan ICT kepada ICTSO dan mengurus penyiasatan atau pemulihan insiden berkaitan; iv. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman atau insiden keselamatan ICT Jabatan; dan v. Mengkaji pembangunan dan pelaksanaan pelan latihan dan program kesedaran keselamatan ICT.	
Pentadbir Sistem ICT adalah terdiri seperti berikut: i. Pentadbir Keselamatan ICT ii. Pentadbir Rangkaian iii. Pentadbir Pusat Data iv. Pentadbir Sistem Aplikasi v. Pentadbir Portal	Pentadbir Sistem ICT

PERKARA	PERANAN
vi. Pentadbir E-mel vii. Pegawai Aset ICT	
i. Melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; ii. Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; iii. Melaporkan ancaman atau insiden keselamatan ICT kepada Pengurus Keselamatan ICT dan seterusnya membantu dalam penyiasatan atau pemulihan; iv. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT; v. Melaporkan sebarang salah laku pengguna yang melanggar Polisi ini kepada Pengurus Keselamatan ICT; dan vi. Menyedia dan melaksanakan pelan latihan dan program kesedaran keselamatan ICT.	Pentadbir Keselamatan ICT

PERKARA	PERANAN
i. Memastikan kemudahan rangkaian beroperasi sepanjang masa; ii. Memastikan semua peralatan dan perisian rangkaian diselenggara dengan sempurna; iii. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; iv. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; dan v. Memantau penggunaan rangkaian dan melaporkan kepada Pentadbir Keselamatan ICT sekiranya berlaku penyalahgunaan sumber rangkaian.	Pentadbir Rangkaian

PERKARA	PERANAN
i. Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; ii. Memastikan keselamatan data dan sistem aplikasi yang berada dalam pusat data; iii. Menjadual dan melaksanakan proses sandaran dan pemulihan (Backup and Restore) ke atas pangkalan data dan sistem secara berkala; iv. Memastikan pusat data sentiasa beroperasi mengikut polisi yang telah ditetapkan; dan v. Melaporkan sebarang pelanggaran keselamatan pusat data kepada Pentadbir Keselamatan ICT.	Pentadbir Pusat Data
i. Memastikan sistem aplikasi mempunyai kawalan capaian; ii. Memastikan data-data rahsia rasmi tidak boleh disalin atau dicetak oleh orang yang tidak berhak; iii. Memastikan reka bentuk sistem aplikasi dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; iv. Melaksanakan pemantauan dan penyelenggaraan terhadap sistem aplikasi dari semasa ke semasa;	Pentadbir Sistem Aplikasi

PERKARA	PERANAN
v. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; dan vi. Melaporkan sebarang pelanggaran keselamatan sistem aplikasi kepada Pentadbir Keselamatan ICT.	
i. Memastikan portal mempunyai kawalan capaian; ii. Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; iii. Memastikan hanya maklumat data terbuka sahaja dipaparkan di portal ; iv. Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; v. Melaksanakan pemantauan dan penyelenggaraan terhadap portal dari semasa ke semasa; vi. Melaporkan sebarang pelanggaran keselamatan portal kepada Pentadbir Keselamatan ICT.	Pentadbir Portal
i. Bertindak sebagai Pentadbir UC di Portal MyGovUC; ii. Melaksanakan proses pengurusan akaun e-mel mengikut prosedur MyGovUC oleh MAMPU;	Pentadbir E-mel

PERKARA	PERANAN
iii. Memastikan kemudahan capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan iv. Melaporkan sebarang pelanggaran keselamatan e-mel kepada Pentadbir Keselamatan ICT.	
i. Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; ii. Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/Bahagian; iii. Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; iv. Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Borang Permohonan Pergerakan/Pinjaman Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/Pegawai Aset/Pegawai-pegawai lain yang diberi kuasa oleh Ketua Jabatan; v. Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/penggantian/naik taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;	Pegawai Aset ICT

PERKARA	PERANAN
vi. Memastikan semua aset ICT Kerajaan dilabel di tempat yang mudah dilihat dan sesuai pada aset berkenaan; vii. Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; dan viii. Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan; ix. Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan x. Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bil. 3 Tahun 2015 ialah merancang dan menentukan langkah-langkah keselamatan ICT.	JPICT
i. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; ii. Merekod dan menjalankan siasatan awal insiden yang diterima;	CERT BHEUU

PERKARA	PERANAN
iii. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; iv. Menasihati Pentadbir Sistem ICT untuk mengambil tindakan pemulihan dan pengukuhan; dan v. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada Pentadbir Sistem ICT.	
i. Membaca, memahami dan mematuhi Polisi ini; ii. Mengetahui dan memahami implikasi keselamatan ICT serta kesan daripada tindakannya; iii. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan; v. Melaksanakan langkah-langkah perlindungan seperti yang berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;	Pengguna

PERKARA	PERANAN
c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan maklumat; e. Mematuhi polisi, piawaian dan garis panduan keselamatan ICT yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan kawalan keselamatan ICT dari diketahui umum. vi. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada CERT BHEUU dengan segera; vii. Menghadiri program-program kesedaran mengenai keselamatan ICT; viii. Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini; dan ix. Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber BHEUU, MdI dan JBG** (**LAMPIRAN 2**).	

PERKARA	PERANAN
2.1.2 PENGASINGAN TUGAS	
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; ii. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; iii. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan aplikasi; dan iv. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
2.1.3 HUBUNGAN DENGAN PIHAK BERKUASA	
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: i. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab Jabatan; ii. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang perlu dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi Dan Multimedia Malaysia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan iii. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	CERT BHEUU/ Pengurusan Sumber Manusia
2.1.4 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS	
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi:	Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
i. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; ii. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; iii. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan iv. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	
2.1.5 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK	
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek Jabatan; ii. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; iii. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;	Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
iv. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam Polisi Keselamatan Siber BHEUU, MdI dan JBG; dan v. Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.	
2.2 PERANTI MUDAH ALIH, TELEKERJA DAN MESYUARAT DALAM TALIAN	
Objektif: Memastikan keselamatan telekerja, mesyuarat dalam talian dan penggunaan peralatan mudah alih.	
2.2.1 POLISI PERANTI MUDAH ALIH	
Membangun serta menyebarkan polisi/arahan/peraturan/langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul berkaitan penggunaan peranti mudah alih.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT
Meluluskan polisi/arahan/peraturan/langkah-langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga Jabatan.	JPICT
Perkara-perkara yang perlu dipatuhi: i. Pendaftaran ke atas peralatan mudah alih;	Warga Jabatan

PERKARA	PERANAN
ii. Keperluan ke atas perlindungan secara fizikal; iii. Kawalan ke atas pemasangan perisian peralatan mudah alih; iv. Kawalan ke atas versi dan *patche*s perisian; v. Sekatan ke atas akses perkhidmatan maklumat secara dalam talian; vi. Kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan vii. Peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.	
2.2.2 TELEKERJA	
i. Polisi/arahan/peraturan/langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja. ii. Kawalan capaian dijalankan bergantung kepada kategori pengguna, sensitiviti aplikasi dan jenis data yang dicapai dan tetapan mudah alih dan telekerja; dan	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Warga Jabatan

PERKARA	PERANAN
iii. Capaian maklumat dan aplikasi di pusat data melalui jarak jauh *(remote access)* adalah terhad kepada pengguna yang dibenarkan sahaja dan mestilah melalui *Virtual Private Network (VPN).*	
2.2.3 MESYUARAT DALAM TALIAN	
Mesyuarat dalam talian hendaklah mengadaptasi teknik yang selamat seperti penggunaan kata laluan sebelum dibenarkan terlibat di dalam mesyuarat berkenaan.	Penyelaras/ Pentadbir Mesyuarat/ Pentadbir Rangkaian
Polisi/arahan/peraturan/langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, dibincang atau disimpan semasa mesyuarat dalam talian.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Warga Jabatan
BIDANG 03 : KESELAMATAN SUMBER MANUSIA	
3.1 SEBELUM PERKHIDMATAN	
Objektif: Memastikan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.	

PERKARA	PERANAN
3.1.1 TAPISAN KESELAMATAN	
Tapisan keselamatan hendaklah dijalankan terhadap warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan ii. Menjalankan tapisan keselamatan untuk warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna
3.1.2 TERMA DAN SYARAT PERKHIDMATAN	
Persetujuan berkontrak dengan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:	Pengguna

PERKARA	PERANAN
i. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan yang terlibat dalam menjamin keselamatan aset ICT; dan ii. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	
3.2 DALAM TEMPOH PERKHIDMATAN	
Objektif : Memastikan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.	
3.2.1 TANGGUNGJAWAB PENGURUSAN	
Pengurusan hendaklah memastikan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Pengguna

PERKARA	PERANAN
3.2.2 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT	
Warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber BHEUU, MdI dan JBG dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; ii. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber BHEUU, MdI dan JBG perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan iii. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Pengguna

PERKARA	PERANAN
3.2.3 PROSES TATATERTIB	
Proses tatatertib yang formal dan disampaikan kepada warga Jabatan hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga Jabatan yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga Jabatan sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh Jabatan; dan ii. Warga Jabatan yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT Jabatan.	Pengurusan Sumber Manusia
3.3 PENAMATAN DAN PERTUKARAN PERKHIDMATAN	
Objektif : Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga Jabatan diurus dengan teratur.	
3.3.1 PENAMATAN ATAU PERTUKARAN TANGGUNG JAWAB PERKHIDMATAN	
Warga Jabatan yang telah tamat perkhidmatan hendaklah: i. Memastikan semua aset ICT dikembalikan kepada Jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;	Warga Jabatan

PERKARA	PERANAN
ii. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan Jabatan dan/atau terma perkhidmatan yang ditetapkan; dan iii. Maklumat rasmi Jabatan dalam peranti tidak dibenarkan dibawa keluar dari Jabatan. Warga Jabatan yang telah bertukar perkhidmatan hendaklah: i. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada Jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan ii. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	
BIDANG 04 : PENGURUSAN ASET	
4.1 TANGGUNGJAWAB TERHADAP ASET	
Objektif: Mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Jabatan.	

PERKARA	PERANAN
4.1.1 INVENTORI ASET	
Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT Jabatan. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: i. Jabatan hendaklah mengenal pasti Pegawai Penerima Aset di setiap Jabatan untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; ii. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan dikemas kini di dalam SPPA mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018 : Tatacara Pengurusan Aset Alih Kerajaan tertakluk kepada perubahan arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; iii. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan iv. Pegawai Aset ICT hendaklah mengesahkan penempatan aset ICT.	Pegawai Aset ICT/Pegawai Penerima Aset/Warga Jabatan
4.1.2 PEMILIKAN ASET	
Aset yang diselanggara hendaklah hak milik Jabatan. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:	Pengurus Keselamatan ICT/Pentadbir

PERKARA	PERANAN
i. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; ii. Memastikan aset telah dikelaskan dan dilindungi; iii. Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; iv. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan v. Memastikan semua jenis aset dipelihara dengan baik.	Sistem ICT/Warga Jabatan
4.1.3 PENGGUNAAN ASET YANG DIBENARKAN	
i. Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan; dan ii. Semua perkakasan ICT persendirian yang dibawa hendaklah mematuhi prosedur keselamatan ICT yang telah ditetapkan oleh Jabatan.	Pengguna
4.1.4 PEMULANGAN ASET	
i. Pengurusan Sumber Manusia hendaklah memaklumkan kepada Pegawai Aset ICT sekiranya terdapat pertukaran pengguna yang diarahkan oleh Ketua Jabatan.	Pengurusan Sumber Manusia/Warga Jabatan

PERKARA	PERANAN
ii. Warga Jabatan hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar kementerian dan penamatan perkhidmatan atau kontrak.	
4.2 PENGELASAN MAKLUMAT (INFORMATION CLASSIFICATION)	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
4.2.1 PENGELASAN MAKLUMAT (CLASSIFICATION OF INFORMATION)	
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan. Maklumat hendaklah dikelaskan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Maklumat hendaklah dikelaskan kepada kategori berikut: i. Maklumat Rahsia Rasmi ii. Maklumat Rasmi iii. Maklumat Pengenalan Peribadi	Pegawai Pengelasan/ Pengguna

PERKARA	PERANAN
iv. Data Terbuka	
4.2.2 PELABELAN MAKLUMAT	
Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Pengguna
4.2.3 PENGENDALIAN ASET	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan,	Pengguna

PERKARA	PERANAN
membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	
4.3 PENGENDALIAN MEDIA	
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
4.3.1 PENGURUSAN MEDIA BOLEH ALIH	
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh Jabatan. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; ii. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; iii. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;	Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
iv. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan v. Menyimpan semua jenis media di tempat yang selamat.	
4.3.2 PELUPUSAN MEDIA	
i. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan ii. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT/ Jawatankuasa yang dilantik untuk pelupusan aset
4.3.3 PEMINDAHAN MEDIA FIZIKAL	
i. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan ii. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem ICT/ Jawatankuasa yang dilantik untuk pelupusan aset

PERKARA	PERANAN
BIDANG 05 : KAWALAN AKSES	
5.1 KAWALAN AKSES	
Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
5.1.1 POLISI KAWALAN AKSES	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: i. Keperluan keselamatan aplikasi; ii. Hak akses dan polisi klasifikasi maklumat sistem dan rangkaian; iii. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;	CIO/ICTSO/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
iv. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; v. Pengasingan peranan kawalan capaian; vi. Kebenaran rasmi permintaan akses; vii. Keperluan semakan hak akses berkala; viii. Pembatalan hak akses; ix. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan x. Capaian *privilege.*	
5.1.2 CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat pengesahan daripada Ketua Jabatan/Bahagian masing-masing. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian Jabatan, rangkaian agensi lain dan rangkaian awam;	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Keselamatan ICT/Pentadbir Rangkaian/ Pengguna

PERKARA	PERANAN
ii. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan iii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
5.2 PENGURUSAN AKSES PENGGUNA	
Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada.	
5.2.1 PENDAFTARAN DAN PEMBATALAN PENGGUNA	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara–perkara berikut hendaklah dipatuhi: i. Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; ii. Akaun ID pengguna mestilah unik; iii. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada Jabatan terlebih dahulu;	Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
iv. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan v. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Jabatan.	
5.2.2 PERUNTUKAN AKSES PENGGUNA	
Satu proses penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT
5.2.3 PENGURUSAN HAK AKSES ISTIMEWA	
i. Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal; dan ii. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada Prosedur Pendaftaran dan Penamatan Pengguna.	Pentadbir Sistem ICT

PERKARA	PERANAN
5.2.4 PENGURUSAN MAKLUMAT PENGESAHAN RAHSIA PENGGUNA	
i. Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal; dan ii. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT
5.2.5 KAJIAN SEMULA HAK AKSES PENGGUNA	
i. Menyemak hak akses pengguna pada sela masa yang ditetapkan; dan ii. Mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT
5.2.6 PEMBATALAN ATAU PELARASAN HAK AKSES	
Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam Jabatan.	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
5.3 TANGGUNGJAWAB PENGGUNA	
Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.	
5.3.1 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA	
i. Membaca, memahami dan mematuhi Polisi Keselamatan Siber BHEUU, MdI dan JBG; ii. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; iii. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat Jabatan; iv. Melaksanakan langkah-langkah perlindungan seperti yang 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;	ICTSO/Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum. v. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan vi. Menghadiri program-program kesedaran mengenai keselamatan ICT.	
5.3.2 PENGGUNAAN MAKLUMAT PENGESAHAN RAHSIA	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	Pentadbir Sistem ICT/Pengguna
5.4 KAWALAN AKSES SISTEM DAN APLIKASI	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	

PERKARA	PERANAN
5.4.1 SEKATAN AKSES MAKLUMAT	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut polisi kawalan capaian.	Pentadbir Sistem Aplikasi/ Pengguna
5.4.2 PROSEDUR LOG MASUK YANG SELAMAT (SECURE LOG-ON)	
Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti berikut: i. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; ii. Mewujudkan kata laluan yang berkualiti; iii. Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; iv. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; v. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; vi. Mewujudkan sistem pengurusan kata laluan berkualiti; dan	Pentadbir Sistem Aplikasi

PERKARA	PERANAN
vii. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
5.4.3 SISTEM PENGURUSAN KATA LALUAN	
Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Jabatan seperti berikut: i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; iv. Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; v. Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; vii. Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan x. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
5.4.4 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA	
Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
5.4.5 KAWALAN AKSES KEPADA KOD SUMBER PROGRAM	
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: i. Log audit perlu dikekalkan kepada semua akses kepada kod sumber; ii. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan iii. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik Jabatan.	Pentadbir Sistem ICT
BIDANG 06 : KRIPTOGRAFI	
6.1 KAWALAN KRIPTOGRAFI	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.	
6.1.1 POLISI PENGGUNAAN KAWALAN KRIPTOGRAFI	
Kriptografi merangkumi kaedah-kaedah seperti berikut: i. Enkripsi Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (encryption).	Pengguna

PERKARA	PERANAN
ii. Tandatangan Digital Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan.	
6.1.2 PENGURUSAN KUNCI AWAM	
Pengurusan ke atas Perkhidmatan Prasarana Kunci Awam (Public Key Infrastructure (PKI)) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah, dikongsi dan didedahkan sepanjang tempoh sah kunci tersebut.	Pentadbir Sistem ICT/Pengguna
BIDANG 07 : KESELAMATAN FIZIKAL DAN PERSEKITARAN	
7.1 KAWASAN SELAMAT	
Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat Jabatan.	
7.1.1 PERIMETER KESELAMATAN FIZIKAL	
Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT Jabatan. Perkara-perkara yang perlu dipatuhi seperti berikut: i. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk	CGSO/Pengarah Seksyen/ Pengurusan Sumber Manusia

PERKARA	PERANAN
melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; ii. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; iii. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; iv. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; v. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; vi. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan vii. Memasang alat penggera atau kamera keselamatan.	

PERKARA	PERANAN
7.1.2 KAWALAN KEMASUKAN FIZIKAL	
Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Jabatan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Warga Jabatan hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada Jabatan apabila bertukar, tamat perkhidmatan atau bersara; ii. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; iii. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT Jabatan; iv. Kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa; dan v. Mematuhi prosedur, peraturan dan polisi sedia ada dalam memasuki ruang kerja di kawasan larangan seperti pusat data, ruang baik pulih perkakasan komputer dan lain-lain ruang yang memerlukan pengawasan dan pemantauan yang khusus.	Pengurusan Sumber Manusia/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
7.1.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; ii. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan iii. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan.	Pengurusan Sumber Manusia/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
7.1.4 PERLINDUNGAN DARIPADA ANCAMAN LUAR DAN PERSEKITARAN	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. Jabatan perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	CIO/ICTSO Pengarah Seksyen/ Pengurusan Sumber Manusia/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
7.1.5 BEKERJA DI KAWASAN SELAMAT	
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga Jabatan yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis Jabatan termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: i. Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik *server* atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; ii. Akses adalah terhad kepada warga Jabatan yang telah diberi kuasa sahaja dan dipantau pada setiap masa; iii. Pemantauan dibuat menggunakan rakaman kamera CCTV atau lain-lain peralatan yang sesuai; iv. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;	Pengarah Seksyen/ Pengurusan Sumber Manusia/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
v. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; vi. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; vii. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; viii. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; ix. Memperkukuh dinding dan siling; dan x. Mengehadkan jalan keluar masuk.	
7.1.6 KAWASAN PENYERAHAN DAN PEMUNGGAHAN	
i. Titik kemasukan *access point* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan; dan ii. Jabatan hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	Pengarah Seksyen/ Pengurusan Sumber Manusia/ Pengguna

PERKARA	PERANAN
7.2 PERALATAN ICT	
Objektif: Melindungi peralatan ICT Jabatan daripada kehilangan, kerosakan, kecurian dan disalahgunakan.	
7.2.1 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT	
Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: i. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; ii. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; iii. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; iv. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
v. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; vi. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna; vii. Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; viii. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set); ix. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; x. Peralatan rangkaian seperti *switch*, *router*, *hub* dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; xi. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;	

PERKARA	PERANAN
xii. Peralatan ICT yang hendak dibawa ke luar premis Jabatan, perlulah mendapat kelulusan Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan; xiii. Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; xiv. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; xv. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir Sistem ICT; xvi. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih; xvii. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; xviii. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;	

PERKARA	PERANAN
xix. Pengguna dilarang sama sekali mengubah password *administrator* yang telah ditetapkan oleh pihak ICT; dan xx. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan Jabatan sahaja.	
7.2.2 UTILITI SOKONGAN	
i. Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan; dan ii. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Pengarah Seksyen/ Pengurusan Sumber Manusia/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
7.2.3 KESELAMATAN KABEL	
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengurusan Sumber Manusia

PERKARA	PERANAN
i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan iv. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	
7.2.4 PENYELENGGARAAN PERALATAN	
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: i. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; ii. Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
iii. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; iv. Melaksanakan prosedur sandaran (data, maklumat, polisi dan konfigurasi) sebagai langkah pencegahan dan alternatif bagi penyelesaian secara *rollback*. v. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan vi. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
7.2.5 PENGALIHAN ASET	
Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: i. Peralatan ICT yang hendak dibawa keluar dari premis Jabatan untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pengarah atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pegawai Aset ICT/Pengguna

PERKARA	PERANAN
ii. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	
7.2.6 KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis Jabatan. Peralatan yang dibawa keluar dari premis Jabatan adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: i. Peralatan perlu dilindungi dan dikawal sepanjang masa; ii. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan iii. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Pengguna
7.2.7 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN	
Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan dan ditempatkan di Jabatan.	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
Peralatan ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Jabatan. Langkah-langkah seperti berikut hendaklah diambil: i. Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; ii. Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; iii. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; iv. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; v. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi;	

PERKARA	PERANAN
b. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Central Processing Unit* (CPU) seperti *Random Access Memory* (RAM), *Hardisk*, *Motherboard* dan sebagainya; c. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian di Jabatan; d. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan e. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Jawatankuasa yang dilantik untuk pelupusan aset Jabatan. vi. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau thumbdrive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; vii. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat Salinan. Penyimpanan *bookmark*, akaun dan kata	

PERKARA	PERANAN
laluan secara terus di memori juga perlu diberi perhatian yang sama; viii. Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa; ix. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan x. Pegawai Aset ICT bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam SPPA.	
7.2.8 PERALATAN PENGGUNA TANPA KAWALAN	
Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: i. Tamatkan sesi aktif apabila selesai tugas; ii. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan	Pengguna

PERKARA	PERANAN
iii. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	
7.2.9 POLISI MEJA KOSONG DAN SKRIN KOSONG	
Polisi meja kosong untuk kertas dan media penyimpanan boleh alih serta polisi skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti berikut: i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat; iv. E-mel masuk dan keluar hendaklah dikawal; dan	Pengarah Seksyen/ Pengguna

PERKARA	PERANAN
v. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	
BIDANG 08 : KESELAMATAN OPERASI	
8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI	
Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.	
8.1.1 PROSEDUR OPERASI YANG DIDOKUMENKAN	
Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: i. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; ii. 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	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
iii. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	
8.1.2 PENGURUSAN PERUBAHAN	
Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: i. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; ii. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; iii. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan	Pentadbir Sistem ICT

PERKARA	PERANAN
iv. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
8.1.3 PENGURUSAN KAPASITI	
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan ii. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem Aplikasi
8.1.4 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI	
Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem ICT

PERKARA	PERANAN
i. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai operasi/pengeluaran (production); ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan iii. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	
8.2 PERLINDUNGAN DARIPADA PERISIAN HASAD (MALWARE)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
8.2.1 KAWALAN DARIPADA PERISIAN HASAD (MALWARE)	
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 dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
i. Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; iv. Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini; v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; vi. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; dan vii. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.	

PERKARA	PERANAN
8.3 SANDARAN (BACKUP)	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
8.3.1 SANDARAN MAKLUMAT	
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat beroperasi 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 yang berikut: i. Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu; ii. Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; iii. Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan	Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
iv. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya TIGA (3) GENERASI.	
8.4 PENGELOGAN DAN PEMANTAUAN (LOGING AND MONITORING)	
Objektif: Merekodkan peristiwa dan menghasilkan bukti.	
8.4.1 PENGELOGAN KEJADIAN (EVENT LOGGING)	
Log peristiwa (event log) yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem (system log) ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi semua maklumat termasuk 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: i. Fail log sistem pengoperasian;	Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
ii. Fail log servis (contoh: web, e-mel); iii. Fail log aplikasi (audit trail); dan iv. Fail log keselamatan (contoh: firewall). Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; ii. Menyemak sistem log secara berkala bagi mengesan ralat dan aktiviti-aktiviti yang tidak normal yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan iii. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CERT BHEUU.	
8.4.2 PERLINDUNGAN MAKLUMAT LOG	
Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.	Pentadbir Sistem ICT

PERKARA	PERANAN
8.4.3 LOG PENTADBIR DAN PENGENDALI	
Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap seperti berikut: i. Memantau penggunaan kemudahan memproses maklumat secara berkala; ii. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; iii. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; iv. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan v. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CERT BHEUU.	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/CERT BHEUU

PERKARA	PERANAN
8.4.4 PENYERAGAMAN JAM (TIME SYNCHRONIZATION)	
i. Aktiviti jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal; dan ii. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan atau domain keselamatan perlu diseragamkan dengan sumber waktu mengikut Malaysian Standard Time (MST) – SIRIM.	Pentadbir Pusat Data
8.5 KAWALAN PEMASANGAN PERISIAN	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
8.5.1 PEMASANGAN PERISIAN PADA SISTEM PENGOPERASIAN	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem pengoperasian. Langkah- langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti berikut: i. Strategi sandaran (backup) perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;	Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
ii. Aplikasi dan sistem pengoperasian hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; iii. Strategi *rollback* perlu dilaksanakan jika perubahan ke atas konfigurasi, sistem dan perisian tidak berjaya; dan iv. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	
8.6 PENGURUSAN KERENTANAN TEKNIKAL	
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.6.1 PENGURUSAN KERENTANAN TEKNIKAL	
Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan sistem operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan sistem operasi;	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/CERT BHEUU

PERKARA	PERANAN
ii. Menganalisis tahap risiko kerentanan; dan iii. Mengambil tindakan pengolahan dan kawalan risiko.	
8.6.2 SEKATAN KE ATAS PEMASANGAN PERISIAN	
Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan. ii. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan iii. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
8.7 PERTIMBANGAN TENTANG AUDIT SISTEM MAKLUMAT	
Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.	

PERKARA	PERANAN
8.7.1 KAWALAN AUDIT SISTEM MAKLUMAT	
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas perkhidmatan ICT di Jabatan.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT
BIDANG 09 : KESELAMATAN KOMUNIKASI	
9.1 PENGURUSAN KESELAMATAN RANGKAIAN	
Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.	
9.1.1 KAWALAN RANGKAIAN	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti berikut: i. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; ii. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna

PERKARA	PERANAN
iii. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; iv. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi; v. *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Keselamatan ICT; vi. Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan Jabatan; vii. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna **KECUALI** mendapat kebenaran daripada ICTSO; viii. Memasang perisian *Intrusion Prevention System (IPS)* bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Jabatan; ix. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; x. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan adalah tidak dibenarkan;	

PERKARA	PERANAN
xi. Semua pengguna perlu menggunakan rangkaian rasmi Jabatan; xii. Penggunaan rangkaian luar perlulah mematuhi prosedur keselamatan ICT yang telah ditetapkan oleh Jabatan; dan xiii. Menggunakan *Virtual Private Network* (VPN) bagi mengelakkan data dan maklumat Jabatan terdedah sewaktu melayari internet, terutamanya apabila menggunakan rangkaian luar.	
9.1.2 KESELAMATAN PERKHIDMATAN RANGKAIAN	
Pengurusan bagi semua perkhidmatan rangkaian yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam dokumen perjanjian.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT
9.1.3 PENGASINGAN DALAM RANGKAIAN	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Jabatan.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
9.2 PEMINDAHAN DATA DAN MAKLUMAT	
Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara Jabatan dan pihak luar terjamin.	
9.2.1 POLISI DAN PROSEDUR PEMINDAHAN DATA DAN MAKLUMAT	
Perkara yang perlu dipatuhi adalah seperti berikut: i. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; ii. Terma pemindahan data, maklumat dan perisian antara Jabatan dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; iii. Media yang mengandungi maklumat perlu dilindungi; dan iv. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pengarah Seskyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
9.2.2 PERJANJIAN MENGENAI PEMINDAHAN DATA DAN MAKLUMAT	
Jabatan perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan	CIO/ICTSO/ Pengarah Seksyen/

PERKARA	PERANAN
data dan maklumat organisasi antara Jabatan dengan pihak luar. Perkara yang perlu dipertimbangkan ialah: i. Pengarah Seksyen hendaklah mengawal penghantaran dan penerimaan maklumat Jabatan; ii. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat Jabatan; iii. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan iv. Jabatan hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan dan data dalam simpanan bagi menghalang ketirisan data.	Pengurus Keselamatan ICT/Pentadbir Sistem ICT
9.2.3 PESANAN ELEKTRONIK (E-MEL)	
Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian e-mel dan undang-undang bertulis lain yang berkuat kuasa adalah seperti berikut:	Warga Jabatan

PERKARA	PERANAN
i. Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003; ii. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet; iii. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; dan iv. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa.	
9.2.4 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN	
i. Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan; dan ii. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO/Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna/ Pembekal

PERKARA	PERANAN
9.2.5 PENGURUSAN PORTAL DAN MEDIA SOSIAL	
i. Memastikan maklumat hebahan (posting) sentiasa disemak atau dikomen (dengan seorang moderator); ii. Menyekat mereka yang terus membuat hebahan atau komen jelik; iii. Melaporkan sebarang pelanggaran polisi penggunaan yang sedang berkuat kuasa; dan iv. Maklumat yang terlibat dalam media sosial hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Peraturan bertulis yang berkuat kuasa adalah: a. Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU); dan b. Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2015 - Pengurusan Laman Web Agensi Sektor Awam.	Pentadbir Portal/Pentadbir Media Sosial/Pengguna

PERKARA	PERANAN
BIDANG 10 : PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.	
10.1.1 ANALISIS DAN SPESIFIKASI KEPERLUAN KESELAMATAN MAKLUMAT	
Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: i. Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan; ii. Semua sistem yang dibangunkan sama ada secara dalaman atau secara *outsources* hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber BHEUU, MdI dan JBG;	Jawatankuasa Penilaian Teknikal/JPICT/ Pentadbir Sistem ICT/Pembekal

PERKARA	PERANAN
iii. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan iv. Ujian keselamatan hendaklah dilakukan semasa pembangunan dan pengujian sistem bagi memastikan kesahihan dan integriti data.	
10.1.2 MELINDUNGI PERKHIDMATAN APLIKASI DALAM RANGKAIAN AWAM	
Maklumat aplikasi yang menggunakan rangkaian awam hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat, pengubahsuaian maklumat yang tidak dibenarkan yang menyebabkan pertikaian kontrak. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Jabatan. Contoh perkhidmatan sumber luaran ialah: a. Perisian Sebagai Satu Perkhidmatan; b. Platform Sebagai Satu Perkhidmatan; c. Infrastruktur Sebagai Satu Perkhidmatan;	Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
d. Storan Pengkomputeran Awan; dan e. Pemantauan Keselamatan. ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; iii. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan *(*authentication*)*; iv. Memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem; v. Memastikan perkhidmatan aplikasi yang melibatkan transaksi data yang sulit menggunakan *Secure Socket Layer* (SSL)*;* vi. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; vii. Memastikan pengguna dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan	

PERKARA	PERANAN
viii. Memastikan tiada halangan atau penduaan maklumat semasa proses pemindahan data dilaksanakan; dan ix. Memastikan pengguna memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	
10.1.3 MELINDUNGI TRANSAKSI PERKHIDMATAN APLIKASI	
Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; ii. Memastikan semua aspek transaksi seperti di bawah dipatuhi: a. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; b. Mengekalkan kerahsiaan maklumat; c. Mengekalkan privasi pihak yang terlibat; dan	ICTSO/Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
d. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. iii. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan; dan iv. Mengaktifkan audit log bagi merekodkan semua transaksi yang melibatkan pengemaskinian data.	
10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi tersebut.	
10.2.1 POLISI PEMBANGUNAN SELAMAT	
Pembangunan perisian dan sistem aplikasi perlu dilaksanakan mengikut keperluan dan ianya hendaklah dikaji dan disemak secara berkala untuk memastikan keberkesanannya.	Pentadbir Sistem ICT
10.2.2 PROSEDUR KAWALAN PERUBAHAN SISTEM	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut:	Pengarah Seksyen/ Pentadbir Sistem ICT

PERKARA	PERANAN
i. Mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan yang ditetapkan dan pelaksanaan hanya mengikut keperluan sahaja; ii. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; iii. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; iv. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; v. Setiap permohonan perubahan/penambahbaikan sistem perlu menggunakan Borang Permohonan Penambahbaikan Sistem (Change Request Form)/Aduan untuk memantau perubahan/penambahbaikan yang dilaksanakan; dan vi. Capaian kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	

PERKARA	PERANAN
10.2.3 KAJIAN SEMULA TEKNIKAL BAGI APLIKASI SELEPAS PERUBAHAN PLATFORM OPERASI	
Apabila platform operasi berubah, semakan dan pengujian perlu dilaksanakan bagi memastikan fungsi dan operasi tidak terjejas. Perkara yang perlu dipatuhi adalah seperti berikut: i. Perubahan platform hendaklah dikaji semasa ke semasa bagi membolehkan ujian yang bersesuaian dapat dilaksanakan; ii. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform; iii. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan iv. Memastikan perubahan yang diselaraskan kepada kesinambungan perkhidmatan.	Pentadbir Sistem ICT
10.2.4 SEKATAN KE ATAS PERUBAHAN DALAM PAKEJ PERISIAN	
Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Memastikan perubahan pakej perisian ini mengambil kira aspek keselamatan maklumat;	Pengarah Seksyen/ Pentadbir Sistem ICT

PERKARA	PERANAN
ii. Perubahan pakej perisian ini hanya dilaksanakan oleh pihak yang dibenarkan sahaja; iii. Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna mengenai perubahan versi pakej perisian; dan iv. Memastikan perubahan pakej perisian ini tidak menjejaskan perkhidmatan operasi sistem maklumat.	
10.2.5 PRINSIP KEJURUTERAAN SISTEM YANG SELAMAT	
Prinsip bagi sistem keselamatan kejuruteraan hendaklah berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini untuk apa-apa usaha pelaksanaan sistem maklumat.	Pengarah Seksyen/ Pentadbir Sistem ICT
10.2.6 PERSEKITARAN PEMBANGUNAN SELAMAT	
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Jabatan perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:	Pengarah Seksyen/ Pentadbir Sistem ICT

PERKARA	PERANAN
i. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; ii. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; iii. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; iv. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; v. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan vi. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	
10.2.7 PEMBANGUNAN OLEH KHIDMAT LUARAN	
Prinsip bagi pembangunan menggunakan khidmat luaran hendaklah berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) dan Garis Panduan Pembangunan Aplikasi Sektor Awam yang terkini untuk apa-apa usaha pembangunan dan pelaksanaan sistem maklumat. Jabatan hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod	ICTSO/Pengarah Seksyen/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
sumber (source code) adalah menjadi **HAK MILIK KERAJAAN**. Perkara yang perlu dipatuhi adalah seperti berikut: i. Perkiraan perlesenan, kod sumber ialah **HAK MILIK KERAJAAN** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara outsource; ii. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori “Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko”; iii. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; iv. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; v. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; vi. Data ujian hendaklah dilupuskan secara kekal (secured delete) selepas projek disiapkan/tamat kontrak; dan	

PERKARA	PERANAN
vii. Aktiviti sandaran hendaklah diuji sehingga berjaya dilakukan sebelum projek tamat.	
10.2.8 PENGUJIAN KESELAMATAN SISTEM	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan ke atas sistem baharu, penambahbaikan sistem, naik taraf dan perubahan versi baharu berdasarkan kriteria yang telah ditetapkan. Bagi memastikan integritI data, pengujian hendaklah dijalankan. Perkara yang perlu dipatuhi adalah seperti berikut: i. Pengujian fungsi keselamatan sistem hendaklah dilaksanakan semasa fasa pembangunan; ii. semua sistem baharu atau penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA); iii. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; iv. Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data;	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
v. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan vi. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	
10.2.9 PENGUJIAN PENERIMAAN SISTEM	
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti berikut: i. Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk 10.1.1 dan 10.1.2) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk 10.2.1); dan ii. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
10.3 DATA UJIAN	
Objektif: Memastikan perlindungan ke atas data yang digunakan untuk pengujian.	

PERKARA	PERANAN
10.3.1 PERLINDUNGAN DATA UJIAN	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal bagi mengelakan data yang diuji tidak tepat. Perkara yang perlu dipatuhi adalah seperti berikut: i. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; ii. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; iii. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan iv. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	ICTSO/Pengurus Keselamatan ICT/Pentadbir Sistem ICT/Pengguna
BIDANG 11 : HUBUNGAN PEMBEKAL	
11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL	
Objektif: Memastikan aset ICT Jabatan yang boleh dicapai oleh pembekal dilindungi.	

PERKARA	PERANAN
11.1.1 POLISI KESELAMATAN MAKLUMAT UNTUK HUBUNGAN PEMBEKAL	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Jabatan. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Mengenal pasti dan mendokumentasi peranan pembekal mengikut tugasan/tanggungjawab; ii. Menyediakan prosedur yang seragam untuk menguruskan pembekal; iii. Mengawal dan memantau akses pembekal; iv. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; v. Jenis-jenis obligasi kepada pembekal; vi. Menyediakan pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; vii. Pembekal perlu mematuhi Arahan Keselamatan yang berkuatkuasa; dan	Pengarah Seksyen/Pemilik Projek/Pembekal

PERKARA	PERANAN
viii. Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber BHEUU, MdI** dan **JBG** (**LAMPIRAN 2**).	
11.1.2 MENANGANI KESELAMATAN DALAM PERJANJIAN PEMBEKAL	
i. 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 organisasi; ii. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak Jabatan selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa; iii. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Jabatan hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian	Pembekal

PERKARA	PERANAN
Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; c. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan CGSO; d. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; e. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; f. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: 1) Badan penilai pihak ketiga adalah bebas dan berintegriti;	

PERKARA	PERANAN
2) Badan penilai pihak ketiga adalah kompeten; 3) Kriteria penilaian; 4) Parameter pengujian; 5) 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 Jabatan; dan h. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Jabatan.	
11.1.3 RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI	
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan ICT serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti berikut: i. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;	Pengarah Seksyen/Pemilik Projek/Pembekal

PERKARA	PERANAN
ii. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan iii. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	
11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL	
Objektif: Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.	
11.2.1 MEMANTAU DAN MENGKAJI SEMULA PERKHIDMATAN PEMBEKAL	
Jabatan hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti berikut: i. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; ii. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan	Pengarah Seksyen/Pemilik Projek/Pembekal

PERKARA	PERANAN
iii. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
11.2.2 MENGURUSKAN PERUBAHAN KEPADA PERKHIDMATAN PEMBEKAL	
Perubahan kepada peruntukan perkhidmatan oleh pembekal termasuk mempertahan dan menambah baik polisi keselamatan maklumat sedia ada, prosedur dan kawalan hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem dan proses bisnes yang terlibat serta penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti berikut: i. Perubahan dalam perjanjian dengan pembekal; ii. Perubahan yang dilakukan oleh Jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian polisi dan prosedur; dan iii. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengarah Seksyen/Pemilik Projek/Pembekal

PERKARA	PERANAN
BIDANG 12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT	
12.1 PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT DAN PENAMBAHBAIKAN	
Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	
12.1.1 TANGGUNGJAWAB DAN PROSEDUR	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden Jabatan adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CERT BHEUU yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: i. Memberikan kesedaran berkaitan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CERT BHEUU dan hebahan kepada warga Jabatan sekiranya ada perubahan; dan ii. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO/Pengarah Seksyen/ CERT BHEUU/ Pengurus Keselamatan ICT/Pentadbir Sistem ICT

PERKARA	PERANAN
12.1.2 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT	
i. Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CERT BHEUU. CERT BHEUU kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Maklumat didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Makumat disyaki hilang dan didedahkan kepada kepada pihak-pihak yang tidak diberi kuasa; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; e. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; f. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan	ICTSO/Pengarah Seksyen/CERT BHEUU

PERKARA	PERANAN
g. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka. ii. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
12.1.3 PELAPORAN KELEMAHAN KESELAMATAN MAKLUMAT	
Warga Jabatan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat Jabatan dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Pengguna/ Warga Jabatan
12.1.4 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT	
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
12.1.5 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT	
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden	ICTSO/CERT BHEUU

PERKARA	PERANAN
keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan ICT CERT BHEUU. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: i. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; ii. Menjalankan kajian forensik sekiranya perlu; iii. Menghubungi pihak yang berkenaan dengan secepat mungkin; iv. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; v. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; vi. Menyediakan pelan kontigensi dan mengaktifkan PKP; vii. Menyediakan tindakan pemulihan segera; dan	

PERKARA	PERANAN
viii. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	
12.1.6 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT	
i. Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya; dan ii. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO/CERT BHEUU
12.1.7 PENGUMPULAN BAHAN BUKTI	
Jabatan hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO/CERT BHEUU

PERKARA	PERANAN
BIDANG 13 : ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
13.1 KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes Jabatan.	
13.1.1 PERANCANGAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Jabatan perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Jabatan. Jabatan juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Melantik pasukan tadbir urus PKP Jabatan; ii. Menetapkan polisi PKP; iii. Mengenal pasti perkhidmatan kritikal;	Ketua Pengarah/ Pengarah Seksyen/ Koordinator PKP/ Pasukan Tindak Balas Kecemasan/ Pasukan Komunikasi Krisis/Pasukan Pemulihan Bencana ICT

PERKARA	PERANAN
iv. Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; v. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana ICT; dan vi. Melaksanakan program kesedaran dan latihan pasukan PKP dan warga Jabatan.	
13.1.2 PELAKSANAAN KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti berikut: i. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal Jabatan yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan dan Pelan Pemulihan Bencana ICT terkini; ii. Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP;	Koordinator PKP/ Pasukan Tindak Balas Kecemasan/ Pasukan Komunikasi Krisis/Pasukan Pemulihan Bencana ICT /CERT BHEUU

PERKARA	PERANAN
iii. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal Jabatan; iv. Mengemas kini struktur tadbir urus PKP Jabatan jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan v. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	
13.1.3 MENENTUSAHKAN, MENGKAJI SEMULA DAN MENILAI KESINAMBUNGAN KESELAMATAN MAKLUMAT	
Jabatan hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pengurusan Atasan Jabatan/ Koordinator PKP/ Pasukan Tindak Balas Kecemasan/ Pasukan Komunikasi Krisis/Pasukan Pemulihan Bencana ICT/Warga Jabatan

PERKARA	PERANAN
13.2 LEWAHAN (REDUNDANCY)	
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.	
13.2.1 KETERSEDIAAN KEMUDAHAN PEMPROSESAN MAKLUMAT	
Kemudahan pemprosesan maklumat Jabatan perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (failover test) keberkesanannya dari semasa ke semasa.	Pengurus Keselamatan ICT/Pentadbir Sistem ICT
BIDANG 14 : PEMATUHAN	
14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN KONTRAK	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
14.1.1 PENGENALPASTIAN KEPERLUAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI	
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga Jabatan, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan. Keperluan perundangan atau	Pengguna

PERKARA	PERANAN
peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna adalah seperti di **LAMPIRAN 1**.	
14.1.2 HAK HARTA INTELEK	
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Pengguna
14.1.3 PERLINDUNGAN REKOD	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Pengguna
14.1.4 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI	
Jabatan hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Pengguna
14.1.5 PERATURAN KAWALAN KRIPTOGRAFI	
Jabatan perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna

PERKARA	PERANAN
i. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi tanpa kelulusan pihak berkuasa; ii. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi tanpa kelulusan pihak berkuasa; iii. Sekatan penggunaan enkripsi yang tidak dibenarkan; dan iv. Mematuhi kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	
14.2 KAJIAN SEMULA KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur Jabatan.	
14.2.1 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI	
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengarah Seksyen/Pemilik Perkhidmatan

PERKARA	PERANAN
14.2.2 PEMATUHAN POLISI DAN STANDARD KESELAMATAN	
Jabatan hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	Pengarah Seksyen/Pemilik Perkhidmatan
14.2.3 KAJIAN SEMULA PEMATUHAN TEKNIKAL	
Jabatan hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	Pengarah Seksyen/Pemilik Perkhidmatan

LAMPIRAN 1

SENARAI PERUNDANGAN DAN PERATURAN

1. Akta Rahsia Rasmi 1972;

2. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama) - “Tatacara Penyediaan, Penilaian dan PenerimaanTender”;

3. Surat Pekeliling Perbendaharaan Bil. 3/1995 - “Peraturan Perolehan Perkhidmatan Perundingan”;

4. Akta Tandatangan Digital 1997;

5. Akta Jenayah Komputer 1997;

6. Akta Hak Cipta (Pindaan) Tahun 1997;

7. Akta Komunikasi dan Multimedia 1998;

8. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;

9. Surat Akujanji (Pekeliling Perkhidmatan Bilangan 17 Tahun 2001);

10. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

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

12. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";

13. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

14. Surat Pekeliling Am Bil. 4 Tahun 2006 – "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";

15. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";

16. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat" bertarikh 30 April 2007;

17. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi – Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC);

18. Arahan Teknologi Maklumat 2007;

19. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";

20. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk “Penggunaan Media Jaringan Sosial di Sektor Awam”;

21. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2013 Dalam Sektor Awam;

22. Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 bertajuk “Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]” bertarikh 23 Oktober 2015;

23. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;

24. Arahan Keselamatan (Semakan dan Pindaan 2017);

25. Myportfolio (Pekeliling Kemajuan Pentadbiran Awam Bil 4 Tahun 2018);

26. Pekeliling Perkhidmatan Bilangan 5 Tahun 2020. Dasar Bekerja Dari Rumah;

27. Arahan Pentadbiran Ketua Pengarah MAMPU Bilangan 4 Tahun 2020 - Polisi Keselamatan Siber MAMPU;

28. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2001 bertajuk “Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam” bertarikh 10 Jun 2021;

29. Perintah-Perintah Am;

30. Arahan Perbendaharaan;

LAMPIRAN 2

SURAT AKUAN
PEMATUHAN POLISI KESELAMATAN SIBER
BAHAGIAN HAL EHWAL UNDANG-UNDANG (BHEUU),
JABATAN INSOLVENSI MALAYSIA (MdI) DAN JABATAN BANTUAN GUAMAN (JBG)

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Bahagian Hal Ehwal Undang-Undang, Jabatan Insolvensi Malaysia dan Jabatan Bantuan Guaman; 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

.....
Pegawai Keselamatan ICT
b.p. Ketua Pengarah BHEUU

.....
(Tarikh)