POLISI KESELAMATAN SIBER

JABATAN LAUT MALAYSIA

PPISMS-UTMKE-01



www.marine.gov.my

KANDUNGAN

01	**TUJUAN**	3
02	**LATAR BELAKANG**	4
03	**OBJEKTIF**	5
04	**GLOSARI**	6-7
05	**PENYATA POLISI KESELAMATAN SIBER JLM**	8
06	**ASET ICT JLM**	9-11
07	**RISIKO**	12
08	**PRINSIP KESELAMATAN**	13-15
09	**BIDANG KESELAMATAN** • BIDANG A.5 KAWALAN ORGANISASI • BIDANG A.6 KAWALAN MODAL INSAN • BIDANG A.7 KAWALAN FIZIKAL • BIDANG A.8 KAWALAN TEKNOLOGI	16-75
10	**LAMPIRAN A - SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN YANG BERKUAT KUASA**	76-78
11	**LAMPIRAN B - SENARAI AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JLM**	79
12	**LAMPIRAN D - BORANG PERAKUAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 (AKTA 88)**	80
13	**LAMPIRAN E - BORANG PERAKUAN APABILA TAMAT KONTRAK BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 (AKTA 88)**	81



1. TUJUAN

Polisi Keselamatan Siber (PKS) Jabatan Laut Malaysia (JLM) ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi oleh semua warga JLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan yang ditawarkan di JLM. Polisi ini juga menerangkan peranan semua pengguna di JLM mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

2. LATAR BELAKANG

PKS ini dibangunkan selaras dengan keperluan ISO/IEC 27001:2022 Information Security Management System (ISMS) yang merupakan amalan terbaik ISO/IEC 27000 dan piawaian antarabangsa dalam menetapkan keperluan secara berterusan sistem pengurusan keselamatan maklumat mengikut konteks organisasi.



3. OBJEKTIF

a Menerangkan kepada semua pengguna merangkumi warga JLM, pembekal/perunding dan pihak yang mempunyai urusan dengan perkhidmatan JLM mengenai tanggungjawab dan peranan mereka dalam melindungi keselamatan maklumat;

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

c Memastikan kelancaran operasi JLM dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

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

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

4. GLOSARI

SINGKATAN/ PERKATAAN	DEFINISI
Aset Tak Ketara	Aset Tak Ketara ialah aset bukan kewangan yang dapat dikenal pasti tanpa kewujudan secara fizikal. Aset Tak Ketara meliputi pelbagai kategori seperti paten, cap dagangan, petunjuk geografi, rekabentuk perindustrian, hak cipta, rekabentuk susun atur litar bersepadu, perlindungan varieti baru tumbuhan, pengetahuan tradisional dan penzahiran kebudayaan, pangkalan data, perjanjian perlesenan, perjanjian hak eksklusif/ hak lokasi mengguna Aset Tak Ketara.1
Backup	Backup merupakan suatu proses menyalin semula data atau sistem dalam komputer/server dan menyimpannya di storan sekunder seperti pendrive, CD dan lain-lain.
CDO	Ketua Pegawai Digital *(Chief Digital Officer)*
CSIRT *(Computer Security Incident Response Team)*	Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu JLM menguruskan pengendalian insiden keselamatan ICT.
ICT	*Information and Communication Technology*
ICTSO	Pegawai Keselamatan ICT *(ICT Security Officer)*
ISMS	Sistem Pengurusan Keselamatan Maklumat *(Information Security Management Systems)*
Klasifikasi	Pembahagian kepada beberapa kategori / pengkelasan berdasarkan kepada Prosedur Kawalan Dokumen dan Rekod atau garis panduan yang ditetapkan.
LAN	LAN *(Local Area Network)* atau Rangkaian Kawasan Setempat adalah sebuah sistem rangkaian yang mempunyai peranti untuk berhubung di antara satu dengan yang lain di dalam rangkaian geografi yang agak terhad jaraknya. Ia hanyalah meliputi sebuah bangunan atau beberapa bahagian kawasan yang berdekatan

SINGKATAN/ PERKATAAN	DEFINISI
MATRAIN	Institut Latihan Pengangkutan Laut
Pegawai Aset	Bertanggungjawab mengurus aset mengikut peraturan yang telah ditetapkan dan menyediakan laporan pengurusan aset.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuatkuasa.
Pemilik Sistem	Bahagian/Unit di JLM yang mempunyai kepentingan terhadap sistem yang dibangunkan.
Pengguna	Warga JLM dan Pihak Ketiga.
Pentadbir Pusat Data	Bertanggungjawab memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat.
Pentadbir Sistem ICT	Bertanggungjawab dalam memastikan sistem-sistem sedia ada beroperasi dengan keadaan baik dan selamat.
Pentadbir Pangkalan Data	Bertanggungjawab dalam memastikan pangkalan data sistem-sistem sedia ada beroperasi dengan keadaan baik dan selamat.
Pentadbir Pangkalan Data	Bertanggungjawab dalam memastikan pangkalan data sistem- sistem sedia ada beroperasi dengan keadaan baik dan selamat.
Pentadbir E-mel	Bertanggungjawab dalam pengurusan e-mel kakitangan JLM.
Pentadbir Pusat Data	Bertanggungjawab dalam memastikan persekitaran fizikal dan keselamatan pusat data serta memastikan pusat data sentiasa beroperasi mengikut prosedur yang telah ditetapkan.
Pentadbir Rangkaian	Bertanggungjawab dalam memastikan rangkaian dan keselamatan rangkaian setempat (LAN) dan rangkaian luas (WAN) di JLM beroperasi sepanjang masa serta berada dalam keadaan baik dan selamat.

1 Pekeliling Perbendaharaan Malaysia – Tatacara Pengurusan Aset Tak Ketara

4. GLOSARI

SINGKATAN/ PERKATAAN	DEFINISI
Peranti Pengkomputeran Peribadi	Peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh: komputer riba, stesen kerja, telefon pintar, tablet, dan peranti storan.
Peranti Rangkaian	Peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti switch, router, firewall, peranti VPN dan kabel.
Restore	Restore ialah proses menyalin data sandaran daripada storan sekunder dan memulihkannya ke lokasi asalnya atau lokasi baharu. Pemulihan dilakukan untuk mengembalikan data yang telah hilang, dicuri atau rosak kepada keadaan asalnya atau untuk memindahkan data ke lokasi baharu.
PKP	Pelan Kesinambungan Perkhidmatan
PKS	Polisi Keselamatan Siber
PYB	Pegawai Yang Bertanggungjawab
Trunking	Sistem pendawaian yang menggunakan sesalur sebagai tempat menyokong dan menyimpan kabel.
UI	Unit Integriti
UP	Unit Perolehan
UPA	Unit Pengurusan Aset
UPKAA	Unit Pengurusan Kewangan dan Akaun Amanah
UPS	*Uninterruptible Power Supply*
UPSM	Unit Pengurusan Sumber Manusia
UTMKE	Unit Teknologi Maklumat dan Kerajaan Elektronik
Unit IT	Unit Teknologi Maklumat di Jabatan Laut Malaysia Wilayah
VPN	*Virtual Private Network*

SINGKATAN/ PERKATAAN	DEFINISI
WAN	WAN *(Wide Area Network)* atau Rangkaian Kawasan Luas merupakan rangkaian komputer jarak jauh dan teknologi yang biasanya digunakan untuk menyambungkan komputer yang berada pada lokasi yang berbeza seperti (negeri, negara & benua).
Wire Tapping	Pengawasan atau perakaman aliran data yang melalui dawai penghantaran suatu sistem perhubungan data.

1 Pekeliling Perbendaharaan Malaysia – Tatacara Pengurusan Aset Tak Ketara

5. PERNYATAAN POLISI KESELAMATAN SIBER JLM

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

Pernyataan ini merangkumi perlindungan ke atas semua maklumat kerajaan samada dalam bentuk elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan dan ketersediaan maklumat tersebut kepada semua pengguna yang dibenarkan.

CIRI-CIRI UTAMA KESELAMATAN MAKLUMAT ADALAH SEPERTI BERIKUT:



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

6. ASET ICT JLM

6.1 ASET ICT JLM

Aset ICT JLM terdiri daripada organisasi, manusia, perisian, peralatan, telekomunikasi, kemudahan ICT, data dan maklumat. JLM telah menetapkan keperluan-keperluan asas keselamatan seperti yang berikut:

1



Data dan maklumat termasuk *hardcopy* dan *softcopy* hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

2



Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan JLM.

6. ASET ICT JLM

PKS JLM merangkumi perlindungan ke atas semua maklumat kerajaan samada dalam bentuk elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan Maklumat

Semua data dan maklumat elektronik dan bercetak yang disimpan atau digunakan di pelbagai media termasuk prosedur, manual pengguna, sistem dokumentasi, rekod, pangkalan data dan lain-lain;

2. Peralatan ICT

Semua peralatan komputer seperti komputer peribadi, komputer riba, pencetak, media storan, *server* dan *firewall*

3. Perisian

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi, perisian sistem, perisian utiliti, sistem pengurusan pangkalan data, kod sumber dan lain-lain;

4. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi- fungsinya. Contoh:
i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, pendingin hawa, sistem pencegah kebakaran dan lain-lain.

5. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif; dan

6. Persekitaran Fizikal

Persekitaran fizikal yang merujuk kepada lokasi fizikal yang menempatkan perkara 1-5 di atas.

6. ASET ICT JLM

6.2 ASET ICT PERSENDIRIAN

Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai maklumat rasmi JLM hendaklah memohon kebenaran daripada pihak UTMKE, JLM. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai maklumat rahsia rasmi dan dilarang sama sekali dibawa masuk ke kawasan terlarang. Teknologi kawalan jauh (remote access) yang boleh menggunakan peranti pengkomputeran peribadi milik persendirian hendaklah dilarang sama sekali.

7. RISIKO

JLM hendaklah melaksanakan pengurusan risiko yang efektif ke atas semua aset ICT yang dikenalpasti. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam kapasiti pengoperasian JLM.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan yang signfikan kepada persekitaran siber JLM.



8. PRINSIP KESELAMATAN

PRINSIP ASAS PKS JLM

1 Prinsip "Perlu-Tahu"

JLM hendaklah melaksanakan mekanisme bagi memberi kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip "Perlu-Tahu" yang memberikan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja. Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkan kepada masa, lokasi dan status bekerja pengguna tersebut.

2 Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah dan menghapuskan sesuatu data atau maklumat.

3 Kebertanggungjawaban atau Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

8. PRINSIP KESELAMATAN

4 Pengasingan Tugas

Tugas mewujud, menghapus, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (unauthorized access) serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi data, operasi, pangkalan data dan rangkaian.

5 Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua log yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit.

6 Pematuhan

PKS JLM hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

7 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui proses backup dan restore serta mewujudkan Pelan Pemulihan Bencana (DRP) di bawah Pelan Kesinambungan Perkhidmatan (PKP).

8. PRINSIP KESELAMATAN

8 **Saling Bergantung**

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

9. BIDANG KESELAMATAN

Empat (4) bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber JLM diterangkan dengan lebih jelas seperti berikut:

BIDANG A.5 KAWALAN ORGANISASI

A.5.1 POLISI KESELAMATAN MAKLUMAT *(POLICIES FOR INFORMATION SECURITY)*	
Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah Laut (KPL) JLM dan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada Ketua Pegawai Digital (CDO), semua Pengarah Bahagian/Wilayah dan Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) serta disokong oleh Mesyuarat Kajian Semula Pengurusan (MKSP) dan Jawatankuasa Kerja ISMS (JKISMS). PKS ini terpakai kepada semua warga JLM dan juga pihak ketiga yang berurusan dengan JLM. Satu set polisi untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan dan disampaikan kepada kakitangan dan pihak luaran yang berkaitan.	KPL, CDO, Pengarah Bahagian/Wilayah, Pengurus ICT, ICTSO, MKSP, JPICT, JKISMS, Warga JLM, Pihak Ketiga

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Peranan dan tanggungjawab Ketua Pengarah Laut adalah seperti berikut: a) Memastikan penguatkuasaan pelaksanaan polisi ini; b) Memastikan warga JLM, pembekal/perunding dan pihak yang mempunyai urusan dengan perkhidmatan JLM memahami dan mematuhi peruntukan-peruntukan di bawah polisi ini; c) Memastikan semua keperluan JLM seperti sumber kewangan, warga JLM dan perlindungan keselamatan adalah mencukupi; d) Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam polisi ini; e) Memastikan pengurusan Pelan Pemulihan Bencana (DRP) di bawah Pelan Kesinambungan Perkhidmatan (PKP) dilaksanakan; dan f) Melantik CDO dan ICTSO.	Ketua Pengarah Laut (KPL)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Ketua Pegawai Digital (CDO) adalah berperanan dan bertanggungjawab : a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam polisi ini; b) Memastikan kawalan keselamatan maklumat JLM diseragam dan diselaraskan dengan sebaiknya; dan c) Menyelaras pelan latihan dan program kesedaran keselamatan ICT.	Ketua Pegawai Digital (CDO)
Pengurus ICT (PICT) adalah berperanan dan bertanggungjawab : a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam polisi ini; b) Memastikan kawalan keselamatan maklumat JLM diseragam dan diselaraskan dengan sebaiknya; dan c) Menyelaras pelan latihan dan program kesedaran keselamatan ICT. d) Melaksanakan keperluan PKS dalam operasi semasa seperti berikut: • Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; • Pembelian atau peningkatan perisian dan sistem komputer; • Perolehan teknologi dan perkhidmatan komunikasi baharu; • Pelantikan pembekal/perunding atau rakan usaha sama; dan • Menentukan pembekal/perunding atau rakan usaha sama menjalani tapisan keselamatan selaras dengan keperluan tahap perkhidmatan. e) Memastikan bentuk ancaman keselamatan terkini dikenal pasti dan penemuan ancaman dilaporkan kepada CDO; f) Menyemak dan mengesahkan garis panduan, prosedur dan tatacara bagi semua aplikasi yang dibangunkan di bahagian-bahagian agar mematuhi keperluan PKS JLM;	Pengurus ICT (PICT)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
g) Membangun, mengkaji semula dan mengemas kini pelan kontingensi dengan mengaktifkan Pelan Pemulihan Bencana (DRP); h) Memastikan sistem kawalan capaian pengguna ke atas aset-aset ICT JLM dilaksanakan; dan i) Memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek.	Pengurus ICT (PICT)
Pegawai Keselamatan ICT (ICTSO) adalah jawatan yang disandang oleh Penolong Pengarah Kanan Seksyen Pengurusan Teknologi, UTMKE. Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) adalah seperti berikut: a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan polisi ini; b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan siber kepada CSIRT JLM dan seterusnya membantu dalam penyiasatan atau pemulihan; e) Melaporkan insiden keselamatan siber kepada Pengurus ICT bagi insiden yang memerlukan Pelan Pemulihan Bencana (DRP) di bawah Pelan Kesinambungan Perkhidmatan (PKP); f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; g) Melaksanakan pematuhan polisi ini oleh warga JLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JLM; h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber;	Pegawai Keselamatan ICT (ICTSO)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber; dan j) Menyelaras pengurusan Pelan Pemulihan Bencana JLM; dan k) Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (Security Posture Assessment, SPA) serta penilaian risiko keselamatan maklumat.	Pegawai Keselamatan ICT (ICTSO)
Peranan dan tanggungjawab Pengarah Bahagian/Wilayah ialah melaksanakan polisi ini dalam operasi semasa seperti berikut: a) Memastikan pihak ketiga dan rakan strategik menjalani tapisan keselamatan; dan b) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi dan pekeliling/garis panduan Kerajaan yang berkuat kuasa.	Pengarah Bahagian/Wilayah
Peranan dan tanggungjawab Mesyuarat Jawatankuasa Pengurusan ISMS (MJKPISMS) adalah menentukan halatuju keseluruhan pelaksanaan pensijilan ISMS JLM yang merangkumi perancangan, pemantauan dan pengesahan terhadap: a) Pelaksanaan pensijilan ISMS ke atas perkhidmatan JLM yang dikenal pasti; b) Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS; c) Penetapan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan*; d) Keputusan dan tindakan Mesyuarat Jawatankuasa Kerja ISMS; e) Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan JLM yang dikenal pasti; f) Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik JLM; g) Keperluan ISMS diterapkan dalam budaya kerja pegawai JLM; h) Sumber yang diperlukan oleh pasukan pelaksana ISMS; i) Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya; j) Pencapaian sasaran ISMS seperti yang dirancang;	Mesyuarat Jawatankuasa Pengurusan ISMS (MJKPISMS)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
k) Arahan dan sokongan kepada Pasukan ISMS JLM bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan l) Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan. i) Memastikan aspek keselamatan maklumat dilaksanakan dalam setiap pengurusan projek. MJKPISMS juga bertanggungjawab untuk meluluskan: a) Struktur organisasi ISMS JLM; b) Keperluan sumber ISMS JLM; dan	Mesyuarat Jawatankuasa Pengurusan ISMS (MJKPISMS)
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Melaksanakan ketetapan sesuatu tahap capaian berdasarkan arahan pemilik sistem/ maklumat; c) Memantau aktiviti capaian sistem aplikasi; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; e) Menganalisis dan menyimpan rekod jejak audit; f) Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala; dan g) Melaporkan sebarang insiden keselamatan sistem ICT kepada CSIRT.	Pentadbir Sistem ICT

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut: a) Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan *Wireless* beroperasi sepanjang masa; b) Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; c) Memastikan polisi/konfigurasi rangkaian yang selamat dilaksanakan; dan d) Memantau penggunaan rangkaian dan melaporkan kepada CSIRT sekiranya berlaku insiden keselamatan rangkaian.	Pentadbir Rangkaian
Peranan dan tanggungjawab Pentadbir Aplikasi/ Pangkalan Data adalah seperti berikut: a) Menguruskan pendaftaran akaun pentadbir/pengguna bagi aplikasi/pangkalan data yang berkaitan; b) Menentukan aplikasi/pangkalan data mematuhi ciri-ciri keselamatan mengikut garis panduan Kerajaan dan piawaian antarabangsa seperti ISO 27002, Code of Practice for Information Security, dan juga garis panduan dan piawaian yang khusus untuk teknologi yang digunakan; c) Memastikan polisi/konfigurasi yang selamat dilaksanakan; d) Merancang dan membuat security update mengikut risiko dan keperluan semasa; e) Membuat pengukuhan (hardening) keselamatan bagi menangani kerentanan sistem aplikasi/pangkalan data yang dikenalpasti; f) Membuat pemantauan dan penyenggaraan ke atas prestasi dan keselamatan aplikasi/pangkalan data secara berkala; dan g) Melaporkan sebarang insiden keselamatan aplikasi/pangkalan data kepada CSIRT.	Pentadbir Aplikasi/ Pangkalan Data

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: a) Menguruskan pendaftaran serta pengurusan e-mel bagi warga JLM; b) Membuat hebahan dan memberi kesedaran berkenaan penggunaan e-mel Jabatan kepada pengguna; dan c) Melaporkan kepada CSIRT atau pihak Jabatan Digital Negara (JDN) sekiranya berlaku keadaan yang luar jangka dan insiden yang berkaitan.	Pentadbir E-mel
Peranan dan tanggungjawab Pentadbir Portal (Web Master) adalah seperti berikut: a) Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b) Memastikan hanya maklumat yang dibekalkan oleh pihak yang berautoriti di paparkan di portal; c) Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; d) Melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server; e) Memantau proses backup dan restoration ke atas kandungan dan aplikasi portal; dan f) Melaporkan sebarang insiden keselamatan portal kepada CSIRT.	Pentadbir Portal (Web Master)
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: a) Memastikan persekitaran fizikal pusat data berada dalam keadaan baik dan selamat; b) Menyediakan Pelan Pemulihan Bencana (DRP) bagi memastikan kesinambungan perkhidmatan;	Pentadbir Pusat Data

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
c) Memastikan pusat data sentiasa beroperasi mengikut prosedur yang telah ditetapkan; dan d) Melaporkan sebarang insiden pelanggaran keselamatan pusat data kepada CSIRT.	Pentadbir E-mel
Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: a) Memastikan aplikasi mematuhi Pelan Stategik Pendigitalan (PSP) serta mengikut pekeliling semasa yang berkuat kuasa; b) Memastikan kesesuaian teknologi dan ciri-ciri keselamatan yang perlu ada bagi aplikasi; c) Memastikan kelancaran operasi sistem dengan meminimumkan risiko keselamatan berkaitan dengan aplikasi; dan d) Memaklumkan penambahan/pertukaran/pembatalan akses pengguna sistem kepada Pentadbir Aplikasi. e) Melaporkan sebarang insiden keselamatan sistem kepada CSIRT.	Pemilik Sistem
Peranan dan tanggungjawab Juruaudit Luaran / Dalaman adalah seperti berikut: a) Menjalankan audit keselamatan bergantung pada skop kerja/ penilaian; b) Menjalankan audit ISMS; c) Menyediakan dan membentangkan laporan penemuan audit kepada MJKPISMS; dan d) Menjalankan audit dalaman dan luaran sekurang-kurangnya satu (1) kali setahun.	Juruaudit Luaran / Dalaman

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT
(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)

Pengguna adalah terdiri dari warga JLM, pembekal/ perunding dan pihak yang mempunyai urusan dengan perkhidmatan JLM. Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Pengguna perlu membaca, memahami dan mematuhi PKS JLM; b) Mengetahui dan memahami implikasi keselamatan maklumat serta kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat JLM; e) Melaksanakan langkah-langkah perlindungan seperti berikut: • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; • Menentukan maklumat sedia untuk digunakan; • Menjaga kerahsiaan kata laluan; • Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan; • Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan,pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan • Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan maklumat kepada CSIRT dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan maklumat; dan h) Mengawal aktiviti penggunaan media sosial seperti di bawah: • Mengelakkan ketirisan maklumat;	Pengguna

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
• Tidak memberi atau mendedahkan sebarang komen atau pernyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan; • Tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau cuba memprovokasi sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan • Tidak menggunakan saluran media sosial hingga mengganggu fokus dalam urusan kerja. i) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JLM seperti di Lampiran B.	Pengguna
Keanggotaan JKISMS adalah seperti berikut: Pengerusi: Pengarah Bahagian Khidmat Pengurusan Penasihat: Pengarah Bahagian Pendaftaran Kapal dan Pengarah MATRAIN Ahli: a) Pengurus ISMS - Ketua Penolong Pengarah (KPP) UTMKE; b) Pasukan Pelaksana : • Ketua Seksyen Pengurusan Teknologi (UTMKE); • Ketua Seksyen Pengurusan Aplikasi (UTMKE) • Wakil Bahagian Perdaftaran Kapal Ibu Pejabat Laut • Wakil Pejabat Pendaftar Kapal:- - JLM Wilayah Tengah, - JLM Wilayah Utara, - JLM Wilayah Labuan, - JLM Wilayah Sabah - JLM Wilayah Sarawak; • Wakil Institut Latihan Pengangkutan Laut (MATRAIN); • Wakil Unit Perolehan; • Wakil Unit Pengurusan Aset; dan • Wakil Unit Pengurusan Sumber Manusia.	Jawatankuasa Kerja ISMS (JKISMS)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Urus setia: Seksyen Pengurusan Pentadbiran (UTMKE) Bidang kuasa: a) Merancang dan menyelaras pensijilan ISMS seperti: • Merancang struktur organisasi ISMS; • Merancang kursus kesedaran ISMS; • Rancang skop ISMS; • Melaksanakan analisis jurang; • Merancang jadual perbatuan ISMS; • Membantu Pelaksana ISMS menyediakan penyataan dasar ISMS, Statement of Applicability (SoA), penilaian risiko,risk treatment plan, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; dan • Permohonan pensijilan. b) Mengemukakan isu dan masalah ISMS, jika ada; dan c) Membantu mengukur keberkesanan kawalan dan pelaksanaan ISMS.	Jawatankuasa Kerja ISMS (JKISMS)
Keanggotaan **CSIRT JLM** adalah seperti berikut: Pengurus: Penolong Pengarah Kanan, UTMKE (Seksyen Pengurusan Teknologi) – ICTSO; Ahli : a) Penolong Pengarah Kanan, UTMKE (Seksyen Pengurusan Aplikasi) b) Penolong Pengarah, UTMKE (Seksyen Pengurusan Teknologi) c) Penolong Pegawai Teknologi Maklumat Kanan, UTMKE (Seksyen Pengurusan Teknologi) d) Penolong Pegawai Teknologi Maklumat, UTMKE (Seksyen Pengurusan Aplikasi)	Pasukan Tindak Balas Insiden Keselamatan ICT JLM (CSIRT JLM)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Peranan dan tanggungjawab CSIRT JLM adalah seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b) Merekod dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menghubungi dan melaporkan insiden yang berlaku kepada Pengurus ICT dan pihak NACSA sama ada sebagai input atau untuk tindakan seterusnya; e) Merujuk Bahagian/ Wilayah di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan f) Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada mesyuarat yang dipengerusikan oleh Pengurusan Tertinggi JLM.	Pasukan Tindak Balas Insiden Keselamatan ICT JLM (CSIRT JLM)
Keanggotaan JKDRP JLM adalah seperti berikut: Pengerusi: Timbalan Ketua Pengarah (Perancangan) – CDO Ahli : a) Ketua Penolong Pengarah, UTMKE b) Penolong Pengarah Kanan, UTMKE (Seksyen Pengurusan Teknologi) ICTSO c) Penolong Pengarah Kanan, UTMKE (Seksyen Pengurusan Sistem Aplikasi); d) Penolong Pengarah, UTMKE (Seksyen Pengurusan Teknologi) e) Penolong Pegawai Teknologi Maklumat, UTMKE (Seksyen Pengurusan Teknologi); f) Penolong Pegawai Teknologi Maklumat, UTMKE (Seksyen Pengurusan Sistem Aplikasi);	Pasukan Tindak Balas Insiden Keselamatan ICT JLM (CSIRT JLM)

A.5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	
Peranan dan tanggungjawab JKDRP JLM adalah seperti berikut: a) Membangunkan Dokumen Pelan Pemulihan Bencana (DRP); b) Menyediakan kemudahan pemulihan bencana atau Pusat Pemulihan Bencana *(Disaster Recovery Centre)*; c) Membuat penilaian ke atas masalah dan jangkaan akibat bencana; d) Memaklumkan pengurusan atasan berkenaan bencana, kemajuan pemulihan bencana dan masalah; e) Mengaktifkan prosedur pemulihan bencana; f) Mengkoordinasi operasi pemulihan; g) Memantau operasi pemulihan dan memastikan jadual pemulihan dipatuhi; h) Mendokumentasikan operasi pemulihan; dan i) Mengkoordinasi simulasi pemulihan bencana.	Jawatankuasa Pelan Pemulihan Bencana (JKDRP) JLM

A.5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubahsuai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalahguna aset JLM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset JLM;	Pengarah Bahagian/ Wilayah

A.5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	
b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset JLM daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	Pengarah Bahagian/ Wilayah

A.5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	
a) Pengurusan atasan JLM hendaklah memastikan semua warga JLM mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan serta mewajibkan pihak yang terlibat dengan Maklumat Rahsia Rasmi menandatangani perjanjian ketakdedahan (non-disclosure) seperti dalam Arahan Keselamatan (Semakan dan Pindaan 2017); dan b) Salinan asal perjanjian / kontrak perkhidmatan dan pembekalan yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.	Ketua Pengarah Laut / Pengarah Bahagian / Pengarah Wilayah/ UPSM / UP

A.5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*	
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab JLM; b) Mewujud dan mengemaskini prosedur / senarai pihak berkuasa. perundangan / pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan adalah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan adalah termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan dan bomba; dan c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	Jawatankuasa Pelan Pemulihan Bencana (JKDRP) JLM

A.5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi: a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga JLM (Mengikut Bidang Kepakaran)

A.5.7 ANCAMAN KECERDASAN *(THREAT INTELLIGENCE)*	
Maklumat berkaitan dengan ancaman keselamatan maklumat hendaklah dikumpul dan dianalisis untuk menghasilkan laporan ancaman kecerdasan.	Pentadbir Sistem ICT

A.5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	
Keselamatan maklumat hendaklah ditangani dalam pengurusan projek, tanpa mengambil kira jenis projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek JLM; b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS JLM.	Warga JLM (Pengurus Projek)

A.5.9 INVENTORI MAKLUMAT DAN ASET YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: a) Memastikan semua aset ICT JLM diberi kawalan dan perlindungan yang sesuai kepada setiap pemilik aset ICT; b) Memastikan semua aset ICT dikenalpasti, dikelaskan, didokumenkan, diselenggarakan dan dilupuskan;	Pegawai Aset/ Pemilik Aset/ Pengguna Aset

A.5.9 INVENTORI MAKLUMAT DAN ASET YANG BERKAITAN *(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
c) Maklumat aset direkodkan dan dikemas kini dalam Sistem Pengurusan Aset (SPA), Kad Daftar Harta Modal dan Aset Alih Bernilai Rendah sebagaimana mengikut Pekeliling Perbendaharaan AM 2 Tahun 2018:Tatacara Pengurusan Aset Alih Kerajaan atau senarai aset yang berkaitan; dan d) Setiap aset mesti mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. e) Senarai aset perlu diselenggara mengikut jadual atau apabila diperlukan (iaitu apabila aset baharu diperolehi atau perubahan besar dalam inventori aset).	Pegawai Aset/ Pemilik Aset/ Pengguna Aset

A.5.10 KEBOLEHGUNAAN MAKLUMAT DAN ASET YANG BERKAITAN *(ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	
Peraturan penggunaan yang dibenarkan bagi maklumat dan aset yang dikaitkan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti, didokumenkan dan dilaksanakan.	Warga JLM

A.5.11 PEMULANGAN ASET *(RETURN OF ASSETS)*	
Semua warga JLM hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Warga JLM/ Seksyen Pengurusan Teknologi/ Unit IT

A.5.12 PENGELASAN MAKLUMAT *(CLASSIFICATION OF INFORMATION)*	
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa berdasarkan keperluan undang-undang, nilai, tahap kritikal dan sensitiviti terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.	Timbalan Ketua Pengarah Perancangan (TKPP)/ Pengarah BKP/ Pegawai Pengelas/ Warga JLM

A.5.13 PELABELAN MAKLUMAT *(LABELLING OF INFORMATION)*	
Prosedur pelabelan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.	Timbalan Ketua Pengarah Perancangan (TKPP)/ Pengarah BKP/ Pegawai Pengelas/ Warga JLM

A.5.14 PEMINDAHAN MAKLUMAT *(INFORMATION TRANSFER)*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan prosedur kawalan pertukaran maklumat yang formal untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b) Melindungi media yang mengandungi maklumat daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari JLM; dan c) Melindungi sebaik-baiknya maklumat yang terdapat di dalam media.	Pengguna

A.5.15 KAWALAN AKSES *(ACCESS CONTROL)*	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Perkara yang mesti dipatuhi termasuk yang berikut: a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c) Undang-undang dan peraturan berkaitan yang berkuat kuasa; d) Pengasingan peranan kawalan capaian; e) Kebenaran rasmi permohonan capaian; f) Keperluan semakan hak capaian secara berkala; g) Pembatalan hak capaian; dan h) Capaian *privilege*.	Pentadbir Sistem ICT

A.5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan pemberian dan pembatalan hak capaian. Perkara–perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh JLM sahaja boleh digunakan; b) Akaun pengguna mestilah unik; c) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada JLM terlebih dahulu;	Pengarah Bahagian/ Wilayah/ Ketua Pejabat/ Pentadbir Sistem ICT/ Pengguna

A.5.16 PENGURUSAN IDENTITI *(IDENTITY MANAGEMENT)*	
d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan dari pihak yang bertanggungjawab.	Pengarah Bahagian/ Wilayah/ Ketua Pejabat/ Pentadbir Sistem ICT/ Pengguna

A.5.17 PENGESAHAN MAKLUMAT *(AUTHENTICATION INFORMATION)*	
Peruntukan maklumat pengesahan rahsia hendaklah dikawal melalui proses pengurusan rasmi. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan.	Pentadbir Sistem ICT/ Pengguna

A.5.18 HAK AKSES *(ACCESS RIGHTS)*	
Pemilik Sistem hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan dan memaklumkan kepada Pentadbir sistem ICT bagi tindakan penetapan semula hak akses pengguna sekiranya terdapat sebarang perubahan.	Pemilik Sistem/ Pentadbir Sistem ICT

A.5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PIHAK KETIGA
(INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS)

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pihak ketiga bagi mengurangkan risiko kepada aset JLM. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Mengenal pasti dan mendokumentasi jenis pihak ketiga mengikut kategori; b) Mengawal dan memantau akses pihak ketiga; c) Keperluan minimum keselamatan maklumat bagi setiap pihak ketiga dinyatakan dalam perjanjian; d) Jenis-jenis obligasi kepada pihak ketiga; e) Pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; f) Mengedar PKS JLM kepada pihak ketiga untuk dibaca, difahami dan dipatuhi; g) Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber JLM- (Lampiran B) h) Menandatangani Borang Akuan Berkaitan Akta Rahsia Rasmi 1972 [Akta 88] – Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-Mana Pihak Yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88] -(Lampiran C) dan; i) Menandatangani Borang Akuan Berkaitan Akta Rahsia Rasmi 1972 [Akta 88] – Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan atau Mana-Mana Pihak Yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88] (Lampiran D)	Pengarah Bahagian/ Wilayah/ Pengurus ICT/ Pihak Ketiga

A.5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PIHAK KETIGA *(ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)*	
a) Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan pihak ketiga yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi; b) Syarikat pihak ketiga hendaklah memastikan semua personel mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam menjalankan perkhidmatan kepada pihak JLM selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa; dan c) Sekiranya syarikat pihak ketiga gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat daripada melaksanakan perkhidmatan tersebut.	Pihak Ketiga

A.5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN PEMBEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI *(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)*	
Perjanjian dengan pihak ketiga hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.	Pengarah Bahagian/ Pihak Ketiga

A.5.22 MEMANTAU DAN MENGKAJI SEMULA PERKHIDMATAN PEMBEKAL *(MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)*	
JLM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pihak ketiga secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pihak ketiga mematuhi perjanjian perkhidmatan; b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pihak ketiga dan mengemukakan status kemajuan; dan c) Memaklumkan mengenai insiden keselamatan kepada pihak ketiga/ pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengarah Bahagian/ Wilayah, Pengurus ICT/ Pentadbir Sistem ICT/ Pihak ketiga

A.5.23 KESELAMATAN MAKLUMAT DALAM PENGKOMPUTERAN DAN SERVIS AWAN *(INFORMATION SECURITY FOR USE OF CLOUD SERVICES)*	
Proses untuk pemerolehan, penggunaan, pengurusan dan keluar daripada perkhidmatan awan hendaklah diwujudkan mengikut keperluan keselamatan maklumat organisasi.	Pentadbir Sistem ICT

A.5.24 PENGURUSAN PERANCANGAN DAN PENYEDIAAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memberi kesedaran berkaitan Prosedur Pelan Pengurusan Bencana ICT dan hebahan kepada warga JLM sekiranya ada perubahan; dan	Pengarah Bahagian/ Wilayah/ Pengurus ICT/ CSIRT JLM/ Pengguna

A.5.24 PENGURUSAN PERANCANGAN DAN PENYEDIAAN INSIDEN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)*	
b) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	Pengarah Bahagian/ Wilayah/ Pengurus ICT/ CSIRT JLM/ Pengguna

A.5.25 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT *(ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS)*	
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	Pengurus ICT/ CSIRT JLM

A.5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT *(RESPONSE TO INFORMATION SECURITY INCIDENTS)*	
a) Insiden keselamatan maklumat hendaklah ditangani berdasarkan prosedur yang didokumenkan; b) Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Pelan Pengurusan Bencana ICT ; c) Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: • Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; • Menjalankan kajian forensik sekiranya perlu; • Menghubungi pihak yang berkenaan dengan secepat mungkin; • Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; • Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; • Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan sekiranya perlu; • Menyediakan tindakan pemulihan segera; dan • Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	Pengurus ICT/ CSIRT JLM

A.5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT *(LEARNING FROM INFORMATION SECURITY INCIDENTS)*	
a) Pengetahuan yang diperolehi daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya; dan b) 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.	Pengurus ICT/ CSIRT JLM

A.5.28 PENGUMPULAN BAHAN BUKTI *A.5.28 PENGUMPULAN BAHAN BUKTI (COLLECTION OF EVIDENCE)*	
JLM hendaklah menentukan prosedur untuk pengumpulan, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	Pengurus ICT/ CSIRT JLM

A.5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN *(INFORMATION SECURITY DURING DISRUPTION)*	
a) JLM hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana; dan b) Dalam merancang kesinambungan keselamatan maklumat, JLM perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi JLM.	Koordinator PKP/ Pasukan Pemulihan Bencana ICT

A.5.30 KETERSEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN *(ICT READINESS FOR BUSINESS CONTINUITY)*	
Ketersediaan ICT hendaklah dirancang, dilaksanakan, diselenggarakan dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT.	Warga JLM (Mengikut Bidang Kepakaran)

A.5.31 PENGENALPASTIAN KEPERLUAN UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI *(IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL AGREEMENT)*	
a) Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga JLM, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JLM; dan b) Pengguna hendaklah mematuhi semua keperluan perundangan atau peraturan-peraturan lain berkaitan seperti **LAMPIRAN A.**	Pengguna

A.5.32 HAK HARTA INTELEK *(INTELLECTUAL PROPERTY RIGHTS)*	
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

A.5.33 PERLINDUNGAN REKOD *(PROTECTION OF RECORDS)*	
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

A.5.34 Privasi dan Perlindungan Maklumat Peribadi *(Privacy And Protection of Personally Identifiable Information)*	
JLM hendaklah memberi jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Pengguna

A.5.35 Kajian Semula Keselamatan Maklumat Secara Berkecuali *(Privacy And Protection of Personally Identifiable Information)*	
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pasukan Audit Dalam/ Audit Luar

A.5.36 PEMATUHAN DASAR, PERATURAN DAN STANDARD KESELAMATAN MAKLUMAT *(COMPLIANCE WITH POLICIES, RULES, AND STANDRDS FOR INFORMATION SECURITY)*	
JLM hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur dalam bidang yang dipertanggungjawabkan terhadap polisi keselamatan, piawaian dan keperluan teknikal yang bersesuaian.	Ketua Pengarah Laut/ CIO/ Pengarah Bahagian/Wilayah/ Pentadbir Sistem ICT

A.5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURES)*	
Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: a) Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;	Pengarah Bahagian/ Wilayah

A.5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN *(DOCUMENTED OPERATING PROCEDURES)*	
b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c) Semua prosedur hendaklah disemak dan dikemaskini dari semasa ke semasa atau mengikut keperluan.	Pengarah Bahagian/ Wilayah

BIDANG A.6 KAWALAN MODAL INSAN

A.6.1 SARINGAN *(SCREENING)*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab semua warga JLM dalam menjamin keselamatan maklumat sebelum, semasa dan selepas perkhidmatan; b) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan surat lantikan yang telah ditetapkan; c) Mendapatkan kelulusan tapisan keselamatan selaras dengan keperluan perkhidmatan; dan d) Memastikan pengguna menandatangani Surat Akuan Pematuhan PKS JLM, lulus Tapisan Keselamatan dan Perakuan Akta Rahsia Rasmi 1972.	UPSM/ Pengguna/ Pembekal/ Perunding

A.6.2 TERMA DAN SYARAT PERKHIDMATAN *(TERMS AND CONDITIONS OF EMPLOYMENT)*	
a) Warga JLM hendaklah mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan surat lantikan yang telah ditetapkan; dan b) Bagi lantikan kontrak hendaklah menandatangani persetujuan semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan surat lantikan yang telah ditetapkan.	UPSM/ Warga JLM/ Pembekal/ Perunding

A.6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESEDARAN MAKLUMAT *(INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING)*	
Warga JLM, pembekal/perunding dan pihak yang mempunyai urusan dengan perkhidmatan JLM perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan maklumat secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan PKS JLM, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/ fungsi/ aplikasi/ sistem keselamatan secara berterusan dalammelaksanakan tugas-tugas dan tanggungjawab mereka; b) Memastikan kesedaran yang berkaitan PKS JLM perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Pengguna/ MATRAIN/ Pengurus ICT

A.6.4 PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	
Proses tatatertib yang formal hendaklah diwujudkan dan disampaikan kepada pengguna bagi membolehkan tindakan diambil terhadap mereka yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan adanya proses tindakan disiplin dan /atau undang-undang ke atas pengguna sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh JLM; dan b) Pengguna yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT JLM.	UI/ UPSM/ Pengguna

A.6.5 PENAMATAN DAN PERTUKARAN TANGGUNGJAWAB PENJAWATAN *(RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT)*	
Warga JLM, pembekal/perunding dan pihak yang mempunyai urusan dengan perkhidmatan JLM yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut: a) Memastikan semua aset ICT milik JLM dikembalikan kepada JLM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b) Membatalkan atau menarik balik semua kebenaran hak capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JLM dan/ atau terma perkhidmatan yang ditetapkan mulai tarikh tamat perkhidmatan; dan c) Maklumat rasmi JLM dalam peranti tidak dibenarkan dibawa keluar dari JLM. Warga JLM yang telah bertukar perkhidmatan hendaklah: a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada JLM mengikut peraturan dan/ atau terma perkhidmatan yang ditetapkan.	UP/ Seksyen Pengurusan Teknologi/ Pengguna
b) Memastikan semua aset ICT milik JLM dikembalikan kepada JLM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan;	Pengarah Bahagian/ Wilayah/ UPSM/ Pengguna

A.6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN *(CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS)*	
a) Syarat-syarat perjanjian kerahsiaan atau non-disclosure perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan; dan b) Pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	UP/ Seksyen Pengurusan Teknologi/ Pengguna

A.6.7 TELEKERJA *(REMOTE WORKING)*	
Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses diproses atau disimpan di lokasi telekerja. Perkara yang perlu dipatuhi bagi memastikan telekerja terjamin adalah seperti berikut: a) Capaian jarak-jauh (working remotely)/ lokasi luar pejabat kepada sistem rangkaian dalaman JLM hendaklah mendapatkan kebenaran terlebih dahulu; dan b) Penghantaran maklumat (SULIT/RAHSIA) yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi *(encryption);* • Lokasi bagi akses ke sistem ICT JLM hendaklah dipastikan selamat; dan • Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan ICT.	Pentadbir Rangkaian/ Pengguna

A.6.8 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	
a) Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin; dan b) Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT JLM. CSIRT JLM kemudiannya perlu melaporkan kepada ICTSO dengan kadar	Pengguna / CSIRT JLM

BIDANG A.7 KAWALAN FIZIKAL

A.7.1 PERIMETER KESELAMATAN FIZIKAL *(PHYSICAL SECURITY PARAMETER)*	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; d) Melaksana perlindungan fizikal dan menyediakan garis panduan untuk pegawai yang bekerja di dalam kawasan terhad; e) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; f) Memasang alat penggera atau kamera keselamatan. g) Mengadakan kaunter kawalan keselamatan; h) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan i) Mewujudkan perkhidmatan kawalan keselamatan.	UPA/ UPSM/ UP/ WPP/ Penolong Pegawai Keselamatan Jabatan (PPKJ)

A.7.2 KEMASUKAN FIZIKAL *(PHYSICAL ENTRY)*	
Kawasan selamat hendaklah dilindungi oleh kawalan kemasukan yang sesuai bagi memastikan pengguna yang diberi kebenaran sahaja dibenarkan masuk. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap warga JLM hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada UPSM apabila bertukar, tamat perkhidmatan atau bersara; b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; c) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT JLM d) Kehilangan pas hendaklah dilaporkan segera kepada Unit Pengurusan Sumber Manusia.	UPSM/ Pengguna

A.7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN *(SECURING OFFICES, ROOMS AND FACILITIES)*	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) 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; b) Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	UPSM/ Pengguna

A.7.4 PEMANTAUAN KESELAMATAN FIZIKAL *(PHYSICAL SECURITY MONITORING)*	
Premis hendaklah sentiasa diawasi daripada sebarang pencerobohan.	BKP

A.7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN *(PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS)*	
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah direka bentuk dan dilaksanakan. JLM perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	Pentadbir Pusat Data/ Jawatankuasa Keselamatan Jabatan

A.7.6 BEKERJA DI KAWASAN SELAMAT *(WORKING IN SECURE AREA)*	
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi semua aset termasuk aset ICT yang terdapat di dalam kawasan tersebut dan termasuklah Pusat Data. Kawalan keselamatan ke atas kawasan tersebut adalah seperti berikut: a) Sumber data atau pelayan (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; b) Akses adalah terhad kepada warga JLM yang telah diberi kuasa sahaja dan dipantau pada setiap masa;	Pentadbir Pusat Data/ UPA

A.7.6 BEKERJA DI KAWASAN SELAMAT *(WORKING IN SECURE AREA)*	
c) Pemantauan dibuat menggunakan Closed-Circuit Television (CCTV) kamera atau lain-lain peralatan yang sesuai; d) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; g) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i) Memperkukuh dinding dan siling; dan j) Mengehadkan jalan keluar masuk	Pentadbir Pusat Data/ UPA

A.7.7 DASAR MEJA BERSIH DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)*	
Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar 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 di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut: a) Menggunakan kemudahan katalaluan *screensaver* atau *logout* apabila meninggalkan komputer;	Warga JLM

A.7.7 DASAR MEJA BERSIH DAN SKRIN KOSONG *(CLEAR DESK AND CLEAR SCREEN)*	
b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Warga JLM

A.7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	
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: a) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; b) Bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; f) Peralatan ICT yang hendak dibawa ke luar premis JLM, perlulah mendapat kelulusan Pegawai Aset/Pembantu Pegawai Aset dan direkodkan bagi tujuan pemantauan; g) Peralatan ICT yang hilang hendaklah dikendalikan mengikut prosedur pelaporan insiden;	Warga JLM/ Unit Pembangunan/ Seksyen Pengurusan Teknologi/ Pegawai Aset/ Pembantu Pegawai Aset

A.7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN *(EQUIPMENT SITING AND PROTECTION)*	
h) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; i) Tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset/Pembantu Pegawai Aset; j) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Seksyen Pengurusan Teknologi untuk dibaik pulih; k) 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; l) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal; m) Pengguna dilarang sama sekali mengubah *password administrator* yang ditetapkan oleh pihak ICT; n) Bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan JLM sahaja; o) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply (UPS)* dan *Generator Set (Gen-Set);* p) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; q) Peralatan rangkaian seperti suis, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; r) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; dan s) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna.	Warga JLM/ Unit Pembangunan/ Seksyen Pengurusan Teknologi/ Pegawai Aset/ Pembantu Pegawai Aset

A.7.9 KESELAMATAN PERALATAN DAN ASET DI LUAR PREMIS *(SECURITY OF EQUIPMENT OFF-PREMISES)*	
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis JLM. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	Warga JLM

A.7.10 MEDIA STORAN *(STORAGE MEDIA)*	
Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengelasan maklumat yang diterima pakai oleh JLM. Prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Memastikan media disimpan dalam persekitaran yang selamat dan terjamin; b) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; c) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; d) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; dan e) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan.	Pemilik Aset/ Pengguna

A.7.10 MEDIA STORAN *(STORAGE MEDIA)*	
Media hendaklah dilupuskan dengan selamat melalui prosedur formal apabila tidak diperlukan lagi. Prosedur pelupusan media adalah seperti berikut: a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan. b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pegawai yang dilantik
Media yang mengandungi maklumat hendaklah dilindungi daripada akses tanpa kebenaran, penyalahgunaan atau kerosakan semasa proses pemindahan.	Pengguna
Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: a) Peralatan ICT yang hendak dibawa keluar dari premis JLM untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan b) Aktiviti peminjaman dan pemulangan perkakasan ICT hendaklah direkodkan oleh Pegawai Aset/Seksyen Teknologi/ Unit IT	Warga JLM/ Pegawai Aset/ Seksyen Pengurusan Teknologi/ Unit IT

A.7.11 UTILITI SOKONGAN *(SUPPORTING UTILITIES)*	
Peralatan ICT hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggarakan dari semasa ke semasa (sekurang-kurangnya setahun sekali).	UPA/ Pentadbir Pusat Data

A.7.12 KESELAMATAN KABEL *(CABLING SECURITY)*	
Kabel bekalan 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: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	UPA/ Pentadbir Rangkaian

A.7.13 PENYELENGGARAAN PERALATAN *(EQUIPMENT MAINTENANCE)*	
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya yang berterusan. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: a) Memastikan setiap perkakasan ICT diselenggara sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; c) Memastikan perkakasan hanya diselenggara oleh PYB atau pihak yang dibenarkan sahaja; d) Menyemak dan menguji perkakasan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Seksyen Teknologi/ UTMKE

A.7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
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 JLM dan ditempatkan di JLM. 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 JLM.	Pegawai Aset/ Pegawai Teknologi Maklumat/ Pembekal

A.7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN
(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)

Langkah-langkah seperti yang berikut hendaklah diambil: a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; e) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut: • Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; • Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *Hardisk*, *Motherboard* dan sebagainya; • iMenyimpan dan memindahkan perkakasan luaran komputer seperti speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di JLM; • Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan • Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JLM. f) Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumbdrive atau external harddisk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; h) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa;	Pegawai Aset/ Pegawai Teknologi Maklumat/ Pembekal

A.7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN *(SECURE DISPOSAL OR RE-USE OF EQUIPMENT)*	
i) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan j) Pegawai aset hendaklah merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset.	Pegawai Aset/ Pegawai Teknologi Maklumat/ Pembekal

BIDANG A.8 KAWALAN TEKNOLOGI

A.8.1 PERANTI POINT-AKHIR PENGGUNA *(USER END-POINT DEVICES)*	
Peranti point-akhir pengguna adalah seperti komputer riba, *tablets*, *Personal Digital Assistances (PDA)*, telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu *Universal Serial Bus (USB)* atau lain-lain peralatan yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik. Perkara yang perlu dipatuhi bagi memastikan keselamatan peranti point-akhir pengguna terjamin adalah seperti berikut: a) Memastikan bahawa kawalan keselamatan yang bersesuaian diambil kira untuk melindungi peranti daripada ancaman keselamatan siber; b) Peralatan point-akhir pengguna hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; c) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan d) Peranti point-akhir pengguna milik persendirian hendaklah dikawal daripada mencapai maklumat Rahsia Rasmi dan hendaklah mematuhi polisi serta prosedur yang ditetapkan untuk dibawa masuk ke kawasan terperingkat.	Pengguna
Pengguna hendaklah memastikan peralatan yang dibiarkan tanpa jagaan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a) Tamatkan sesi aktif apabila selesai tugas; b) *Log-off* komputer apabila sesi bertugas selesai atau tidak lagi digunakan; dan c) Memastikan komputer selamat daripada pengguna yang tidak dibenarkan.	Warga JLM

A.8.2 HAK AKSES ISTIMEWA *(PRIVILEAGE ACCESS RIGHTS)*	
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses istimewa perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pengarah Bahagian/ Wilayah/ Ketua Pejabat/ Pentadbir Sistem ICT

A.8.3 SEKATAN CAPAIAN MAKLUMAT *(INFORMATION ACCESS RESTRICTION)*	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut peraturan/konfigurasi kawalan capaian.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.4 AKSES KEPADA KOD SUMBER PROGRAM *(ACCESS TO SOURCE CODE)*	
Capaian kepada kod sumber program hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan seperti berikut: a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber; b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik JLM.	Pengurus ICT/ Pentadbir sistem ICT/ Pemilik Sistem

A.8.5 PENGESAHAN SELAMAT *(SECURE AUTHENTICATION)*	
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: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan JLM; b) Pendedahan maklumat ketika log masuk mestilah berdasarkan kepada prinsip 'Atas dasar perlu mengetahui'; c) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; d) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; e) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; f) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan g) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	Pentadbir Rangkaian dan Keselamatan ICT

A.8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan kapasiti masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan	Pengurus ICT/ ICTSO/ Pentadbir Sistem ICT/ Pengarah Bahagian/ Wilayah / Unit IT

A.8.6 PENGURUSAN KAPASITI *(CAPACITY MANAGEMENT)*	
b) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus ICT/ ICTSO/ Pentadbir Sistem ICT/ Pengarah Bahagian/ Wilayah / Unit IT

A.8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD *(PROTECTION AGAINST 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 dari perisian berbahaya adalah seperti berikut: a) 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; b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d) Mengemas kini *antivirus* dengan *signature/pattern antivirus* yang terkini; e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) 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.	Seksyen Pengurusan Teknologi/ Pentadbir Sistem ICT

A.8.8 PENGURUSAN KERENTANAN TEKNIKAL *(MANAGEMENT OF TECHNICAL VULNERABILITIES)*	
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 operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Melaksanakan ujian penembusan untuk memperolehi maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; b) Menganalisis tahap risiko kerentanan; dan c) Mengambil tindakan pembetulan dan kawalan risiko.	Seksyen Pengurusan Teknologi/ CSIRT JLM

A.8.9 PENGURUSAN KONFIGURASI *(CONFIGURATION MANAGEMENT)*	
Konfigurasi termasuk konfigurasi keselamatan perkakasan, perisian, perkhidmatan dan rangkaian hendaklah dibangunkan, didokumenkan, dilaksanakan, dipantau serta di semak.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.10 PENGHAPUSAN MAKLUMAT *(INFORMATION DELETION)*	
Maklumat yang disimpan dalam sistem maklumat, peranti atau di storan media yang lain hendaklah dihapuskan apabila tidak diperlukan.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.11 MASKER DATA *(DATA MASKING)*	
Masker data hendaklah digunakan dalam kawalan akses berpandukan dasar, dan keperluan peniagaan yang diambil kira keperluan undang-undang. Penggunaan adalah bergantung kepada deklarasi Statement of Applicability (SOA).	Pengurus ICT/ Pentadbir Sistem ICT

A.8.12 PERLINDUNGAN KETIRISAN DATA *(DATA LEAKAGE PREVENTION)*	
Perlindungan ketirisan data hendaklah dilaksanakan dalam sistem, rangkaian dan lain-lain peranti yang memproses, menyimpan dan mengendali maklumat sensitif.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.13 SANDARAN MAKLUMAT *(INFORMATION OF BACKUP)*	
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di offsite. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi; b) Membangunkan Prosedur Backup and Restoration bagi sistem spesifik (jika perlu);	Pentadbir Sistem ICT

A.8.13 SANDARAN MAKLUMAT *(INFORMATION OF BACKUP)*	
c) Menguji sistem sandaran sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan d) Sandaran hendaklah direkodkan dan disimpan di off-site (lokasi yang berlainan) dan selamat.	Pentadbir Sistem ICT

A.8.14 LEWAHAN KEMUDAHAN PEMPROSESAN MAKLUMAT *(REDUNDANCY OF INFORMATION PROCESSING FACILITIES)*	
Kemudahan pemprosesan maklumat JLM perlu mempunyai redundancy yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan redundancy perlu diuji (failover test) keberkesanannya dari masa ke semasa.	Pentadbir Pusat Data/ Pentadbir Sistem ICT/ Pihak ketiga

A.8.15 PENGELOGAN *(LOGGING)*	
a) Log kejadian yang merekodkan aktiviti pengguna, pengecualian, ralat dan kejadian keselamatan maklumat hendaklah dihasilkan, disimpan dan dikaji semula secara tetap; b) Log sistem ICT adalah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan; c) Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data; dan	Pentadbir Sistem ICT

A.8.15 PENGELOGAN *(LOGGING)*	
d) Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: • Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; • Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan • Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CSIRT JLM.	Pentadbir Sistem ICT

A.8.16 PEMANTAUAN AKTIVITI *(MONITORING ACTIVITIES)*	
Rangkaian, sistem dan aplikasi hendaklah dipantau dari aktiviti (tingkah-laku sistem) yang tidak wajar dan tindakan tertentu harus diambil bagi menilai potensi berlakunya insiden keselamatan maklumat.	Pentadbir Rangkaian

A.8.17 PENYERAGAMAN JAM *(CLOCK SYNCHRONISATION)*	
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi hendaklah diseragamkan mengikut sumber rujukan masa tunggal.	Pentadbir Pusat Data/ Pentadbir Sistem ICT

A.8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA *(USE OF PRIVILEGED UTILITY PROGRAMS)*	
Penggunaan program utiliti yang mungkin mampu melepasi kawalan sistem dan aplikasi hendaklah disekat dan dikawal dengan ketat.	Pentadbir Rangkaian

A.8.19 PEMASANGAN PERISIAN PADA SISTEM YANG BEROPERASI *(INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS) [OK]*	
Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang beroperasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: a) Strategi rollback perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakui berjaya; dan c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	Pengurus ICT / Pentadbir Sistem ICT

A.8.20 KESELAMATAN RANGKAIAN *(NETWORK SECURITY)*	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pegawai ICT perlu membangunkan kawalan yang bersesuaian untuk menghalang capaian tanpa kebenaran yang boleh memberi impak kepada keselamatan maklumat organisasi; b) Memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; c) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; dan d) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja.	Seksyen Pengurusan Teknologi/ Pentadbir Rangkaian/ Pihak Ketiga

A.8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN *(SECURITY OF NETWORK SERVICES)*	
Pengurusan bagi semua perkhidmatan rangkaian *(inhouse* atau *outsource)* yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	Seksyen Pengurusan Teknologi/ Pentadbir Rangkaian dan Pembekal

A.8.22 PENGASINGAN DALAM RANGKAIAN *(SEGREGATION IN NETWORKS)*	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JLM.	Seksyen Pengurusan Teknologi/ Pentadbir Rangkaian

A.8.23 PENAPISAN PORT *(WEB FILTERING)*	
Akses kepada portal luar hendaklah diurus dengan baik bagi mengurangkan keterdedahan kepada kandungan hasad. Perlaksanaan di JLM adalah sebagaimana berikut: a) Memberi pendedahan kepada warga JLM tentang serangan siber yang boleh berlaku melalui capaian portal luar yang tidak selamat b) Organisasi menyekat laman-laman portal yang telah dikenalpasti tidak selamat c) Organisasi juga memberi pendedahan kepada warga JLM jika berlaku capaian portal yang diragui, tindakan seterusnya adalah melaporkan kepada Seksyen Pengurusan Teknologi.	Pengarah Bahagian/ Pentadbir Rangkaian

A.8.24 PENGGUNAAN KRIPTOGRAFI *(USE OF CRYPTOGRAPHY)*	
Polisi penggunaan kawalan kriptografi bagi melindungi maklumat hendaklah dibangunkan dan dilaksanakan. Kriptografi merangkumi kaedah-kaedah seperti berikut: a) Enkripsi - Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat SULIT dan RAHSIA rasmi pada setiap masa. b) Tandatangan digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital (jika ada) mengikut keperluan pelaksanaan.	Pengarah Bahagian/ Pentadbir sistem ICT

A.8.25 KITAR HAYAT PEMBANGUNAN SELAMAT *(SECURE DEVELOPMENT LIFE CYCLE)*	
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; c) Keperluan keselamatan dalam fasa reka bentuk; d) Keperluan pengetahuan ke atas keselamatan aplikasi; e) Keselamatan dalam kawalan versi; dan f) Bagi pembangunan secara outsource, pembekal yang dilantik hendaklah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	Pengurus ICT/ ICTSO/ Pentadbir Sistem ICT

A.8.26 MELINDUNGI PERKHIDMATAN APLIKASI DALAM RANGKAIAN AWAM
(SECURING APPLICATION SERVICES ON PUBLIC NETWORKS)

Maklumat pada aplikasi sistem yang dihantar melalui rangkaian awam hendaklah dilindungi daripada penipuan, pertikaian kontrak dan pendedahan tanpa kebenaran. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Semua perkhidmatan sumber luaran (outsource) hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JLM. Contoh perkhidmatan sumber luaran ialah: • Perisian Sebagai Satu Perkhidmatan (SaaS) • Platform Sebagai Satu Perkhidmatan (PaaS) • Infrastruktur Sebagai Satu Perkhidmatan (IaaS) • Storan Pengkomputeran Awan • Pemantauan Keselamatan b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan *(authentication);* d) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti serahan serta penerimaan dokumen dan kontrak.	Seksyen Pengurusan Teknologi/ Pentadbir Sistem ICT

A.8.27 PRINSIP KEJURUTERAAN SISTEM YANG SELAMAT *(SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES)*	
a) Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat; dan b) Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat JLM.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.28 PENGATURCARAAN SELAMAT *(SECURE CODING)*	
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. JLM perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; dan e) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pengurus ICT/ Pentadbir Sistem ICT

A.8.29 PENGUJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN *(SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE)*	
Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	ICTSO/ Pentadbir Sistem ICT/ Pemilik Sistem

A.8.30 PEMBANGUNAN PERKHIDMATAN LUAR *(OUTSOURCED DEVELOPMENT)*	
JLM hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara outsource oleh pihak luar. Kod sumber (source code) adalah menjadi HAK MILIK JLM.	Pengarah Bahagian/Wilayah, Pengurus ICT/ Pentadbir Sistem ICT

A.8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI *(SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS)*	
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: a) Persekitaraan *(environment)* yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran *(production)*; dan	Seksyen Pengurusan Teknologi/ Pentadbir Sistem ICT

A.8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI *(SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONAL ENVIRONMENTS)*	
b) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.	Seksyen Pengurusan Teknologi/ Pentadbir Sistem ICT

A.8.32 PENGURUSAN PERUBAHAN *(CHANGE MANAGEMENT)*	
Perubahan dalam organisasi, proses perkhidmatan, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur ICT mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	Warga JLM/ Pengurus ICT/ ICTSO/ Pentadbir Sistem ICT/ Pengarah Bahagian/ Wilayah/ UTMKE/ Unit IT Wilayah

A.8.33 PERLINDUNGAN DATA UJIAN *(PROTECTION OF TEST DATA)*	
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	ICTSO/ Pentadbir Sistem ICT/ Pemilik Sistem

A.8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT *(PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING)*	
Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perkhidmatan.	Seksyen Pengurusan Teknologi/ Pentadbir Sistem ICT

10. LAMPIRAN A – SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN YANG BERKUAT KUASA

BIL	SENARAI PERUNDANGAN DAN PERATURAN
1.	Arahan Keselamatan (Semakan dan Pindaan 2017)
2.	Akta Rahsia Rasmi 1972
3.	Akta 629 – Akta Arkib Negara 2003;
4.	Arahan Perbendaharaan (Pindaan 2023);
5.	Arahan Teknologi Maklumat 2007;
6.	Akta Tandatangan Digital 1997;
7.	Akta Hak Cipta (Pindaan) Tahun 1997;
8.	Akta Jenayah Komputer 1997;
9.	Akta Komunikasi dan Multimedia 1998;
10.	Arahan Ketua Pengarah Laut Bilangan 2 Tahun 2020 - Panduan Dan Tatacara Pengurusan Dokumen Rahsia Rasmi Kerajaan Dan Kawalan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat Dan Komunikasi (ICT) Serta Kawalan Rahsia Rasmi Dalam Mesyuarat Kerajaan
11.	Surat Akujanji;
12.	MyPortfolio;
13.	Perintah-Perintah Am;
14.	Pelan Kesinambungan Perkhidmatan;
15.	Garis Panduan Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam (MAMPU);
16.	*Guideline to Determine Information Security Professionals Requirement for the CNII Agencies / Organisations;*
17.	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016, versi 1.0;

10. LAMPIRAN A – SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN YANG BERKUAT KUASA

BIL	SENARAI PERUNDANGAN DAN PERATURAN
18.	*Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002*;
19.	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat yang bertarikh 24 November 2010;
20.	Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022;
21.	Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
22.	Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
23.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
24.	Pekeliling Perbendaharaan 5 Tahun 2207 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
25.	Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
26.	Surat Pekeliling Am Bilangan 3 Tahun 2015 bertajuk "Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek ICT Agensi Sektor Awam";
27.	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";
28.	Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
29.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
30.	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
31.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010; dan
32.	Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

10. LAMPIRAN A – SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN YANG BERKUAT KUASA

BIL	SENARAI PERUNDANGAN DAN PERATURAN
33.	Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
34.	Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
35.	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
36.	Akta-akta/Kaedah/Pekeliling/Arahan lain yang berkaitan.

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JLM

Nama (Huruf Besar) : .....
No. Kad Pengenalan/No. Passport : .....
Jawatan : .....
Bahagian/Wilayah : .....
Nama Organisasi (selain warga JLM) : .....
Nama Kontrak /No. Kontrak : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : .....
Tarikh : .....

Pengesahan Pengarah Bahagian / Wilayah

(.....)
b.p. Ketua Pengarah Laut,
Jabatan Laut Malaysia

Tarikh:

12. LAMPIRAN D – BORANG PERAKUAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan : .....
Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan/ Organisasi : .....
Tarikh : .....
Disaksikan Oleh : .....
(Tandatangan)

Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan/ Organisasi : .....
Tarikh : .....
Cap Jabatan/ Organisasi

13. LAMPIRAN E – BORANG PERAKUAN APABILA TAMAT KONTRAK BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

PERAKUANUNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah Seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana phak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan : .....
Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan/ Organisasi : .....
Tarikh : .....
Disaksikan Oleh : .....
(Tandatangan)

Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Jabatan/ Organisasi : .....
Tarikh : .....
Cap Jabatan/ Organisasi

JABATAN LAUT MALAYSIA

Menara Dius Api, Ibu Pejabat Laut, Jabatan Laut
Malaysia, PT 664, Jalan Limbungan, Kawasan 13,
42007 Port Klang, Selangor