



KEMENTERIAN SUMBER ASLI, ALAM SEKITAR
DAN PERUBAHAN IKLIM
JABATAN ALAM SEKITAR

POLISI KESELAMATAN SIBER

JABATAN ALAM SEKITAR



VERSI 1.0

KANDUNGAN

SEJARAH DOKUMEN POLISI KESELAMATAN SIBER	4
TUJUAN.....	5
LATAR BELAKANG.....	12
OBJEKTIF	12
PEMAKAIAN POLISI	13
TADBIR URUS	14
ASET ICT	15
RISIKO.....	19
PRINSIP KESELAMATAN	22
TEKNOLOGI	23
PROSES	28
MANUSIA.....	30
PELAN PENGURUSAN KESELAMATAN MAKLUMAT	33
PERNYATAAN POLISI KESELAMATAN SIBER JAS	35
BIDANG A.1 : POLISI KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY POLICY</i>)	38
BIDANG A.2 : PERANCANGAN BAGI KESELAMATAN ORGANISASI (<i>ORGANIZATION OF INFORMATION SECURITY</i>).....	40

BIDANG A.3 : KESELAMATAN SUMBER MANUSIA (<i>HUMAN RESOURCE SECURITY</i>)	51
BIDANG A.4 : PENGURUSAN ASET (<i>ASSET MANAGEMENT</i>).....	56
BIDANG A.5 : KAWALAN AKSES (<i>ACCESS CONTROL</i>)	63
BIDANG A.6 : KRIPTOGRAFI (<i>CRYPTOGRAPHY</i>).....	74
BIDANG A.7 : KESELAMATAN FIZIKAL DAN PERSEKITARAN (<i>PHYSICAL AND ENVIRONMENTAL SECURITY</i>)	76
BIDANG A.8 : KESELAMATAN OPERASI (<i>OPERATIONS SECURITY</i>).....	91
BIDANG A.9 : KESELAMATAN KOMUNIKASI (<i>COMMUNICATIONS SECURITY</i>)	103
BIDANG A.10 : PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM (<i>SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE</i>).....	109
BIDANG A.11 : HUBUNGAN PEMBEKAL (<i>SUPPLIER RELATIONSHIP</i>).....	120
BIDANG A.12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (<i>INFORMATION SECURITY INCIDENT MANAGEMENT</i>).....	126
BIDANG A.13 : ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (<i>INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT</i>)	132
BIDANG A.14 : PEMATUHAN (<i>COMPLIANCE</i>)	136

SEJARAH DOKUMEN POLISI KESELAMATAN SIBER

Versi	Tarikh	Ringkasan Semakan / Pindaan
1.0	Jun 2022	Terbitan Pertama

TAKRIFAN

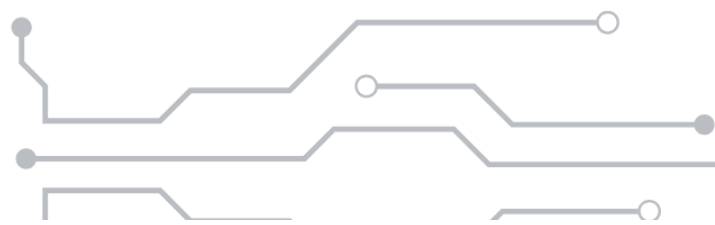
Bagi maksud menjelaskan istilah yang digunakan didalam polisi ini adalah sebagai berikut:

- | | |
|---|---|
| 1) Antivirus | Perisian yang mengimbas virus pada media storan seperti disket cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM untuk sebarang kemungkinan adanya virus. |
| 2) Aset ICT | Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. |
| 3) Aset Alih | Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan. |
| 4) <i>Backup</i> (Sandaran) | Proses penduaan sesuatu dokumen atau maklumat. |
| 5) Saki risiko | Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan. |
| 6) <i>Bandwidth</i> (Jalur lebar) | Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan |
| 7) BCP/PKP | <i>Business Continuity Planning</i>
Pelan Kesyinambungan Perkhidmatan |
| 8) CCTV | <i>Closed-Circuit Television System</i> |
| 9) CIA | <i>Confidentiality, Integrity, Availability</i> |
| 10) CDO | <i>Chief Digital Officer</i>

Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi. |
| 11) <i>Clear Desk</i> dan <i>Clear Screen</i> | Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya. |
| 12) <i>Data-at-rest</i> (data-dalam-simpanan) | Merujuk kepada data yang disimpan dalam sistem destinasi yang stabil. Data dalam simpanan sering ditakrifkan sebagai data yang tidak digunakan atau tidak bergerak ke titik akhir sistem, seperti peranti mudah alih atau stesen kerja. |



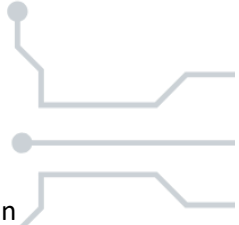
13) <i>Data-in-motion</i> (data-dalam-pergerakan)	Merujuk kepada aliran data yang bergerak melalui sebarang jenis rangkaian. Ia mewakili data yang sedang dipindahkan atau dipindahkan.
14) <i>Data-in-use</i> (data – dalam penggunaan)	Merujuk kepada data yang bukan hanya disimpan secara pasif di destinasi yang stabil, seperti gudang data pusat, tetapi sedang digunakan infrastruktur IT yang lain.
15) <i>Denial of service</i>	Halangan pemberian perkhidmatan.
16) <i>Defence-in-depth</i>	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
17) <i>Downloading</i>	Aktiviti muat turun sesuatu perisian.
18) <i>Encryption</i>	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
19) <i>Escrow</i> (escrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
20) <i>Firewall</i>	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
21) <i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft/espionage</i>), penipuan (<i>hoaxes</i>).
22) ERT JAS	<i>Emergency Response Team</i>
23) <i>Hard disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
24) <i>Hub</i>	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu port kepada semua port yang lain.



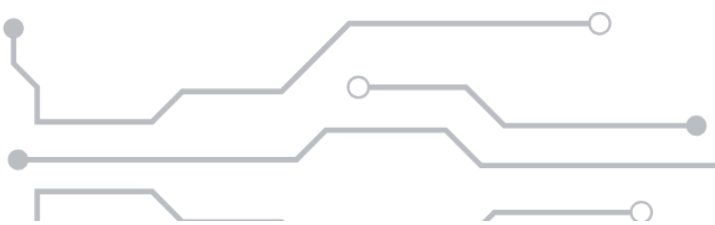


25) ICT	<i>Information and Communication Technology</i> Teknologi Maklumat dan Komunikasi
26) ICTSO	<i>ICT Security Officer</i> Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
27) Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
28) Impak fungsi jabatan	Melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan pelanggaran privasi.
29) Insiden Keselamatan	Musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
30) Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
31) <i>Internet Gateway</i>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik- trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
32) Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau jabatan dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.
33) ISDN	<i>Integrated Services Digital Network</i> Menggunakan isyarat digital pada talian telefon analog yang sedia ada.
34) <i>Intrusion Detection System</i> (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.



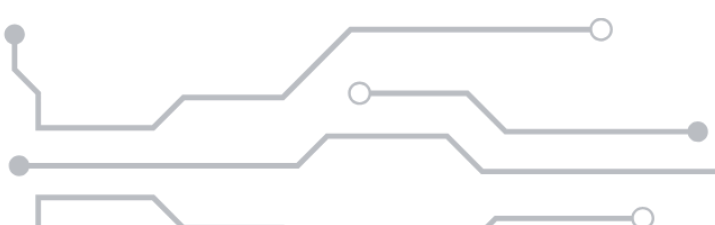


35) <i>Intrusion Prevention System (IPS)</i>	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau <i>malicious code</i> . Contohnya: <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan
36) ISMS	<i>Information Security Management System</i> Sistem Pengurusan Keselamatan Maklumat
37) JAS	Jabatan Alam Sekitar
38) Keadaan Berisiko Tinggi	Dalam situasi yang mudah mendapat ancaman dari pihak luar atau apa-apa kemungkinan yang boleh menjejaskan kelancaran sistem.
39) Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
40) Kriptografi	Kaedah untuk menukar data dan maklumat biasa (<i>standard format</i>) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
41) LAN	<i>Local Area Network</i> Rangkaian Kawasan Setempat yang menghubungkan komputer.
42) <i>Lock</i>	Mengunci komputer
43) <i>Logout</i>	<i>Log-out</i> komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
44) <i>Malicious code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.
45) <i>Mobile code</i>	<i>Mobile code</i> merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh <i>Java Applet</i> , <i>ActiveX</i> dan sebagainya pada pelayar internet.





46) <i>MODEM</i>	<i>MODulator DEModulator</i> Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
47) <i>Outsource</i>	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
48) Pasukan ERT	Pasukan Tindakan Kecemasan/<i>Emergency Response Team</i> (ERT)
49) Pegawai pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
50) Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
51) Perisian Aplikasi	Merujuk kepada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> atau pun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
52) <i>Public-Key Infrastructure</i> (PKI)	Infrastuktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet
53) <i>Rollback</i> (undur)	Pengembalian pangkalan data atau program kepada keadaan stabil sebelum sesuatu ralat berlaku.
54) <i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
55) Ruang siber	Sistem-sistem teknologi maklumat dan komunikasi. Maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT





56) <i>Screensaver</i>	Imej yang akan diaktifkan pada sistem komputer setelah ianya tidak digunakan dalam jangka masa tertentu
57) <i>Server</i>	Pelayan komputer
58) <i>Source Code</i>	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia
59) <i>Switches</i>	Suis merupakan gabungan hab dan titi yang mengasingkan mengikut segmentasi rangkaian
60) <i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
61) <i>Uninterruptible Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
62) <i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna pada masa yang sama ia diterima oleh penghantar.
63) <i>Video Streaming</i>	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
64) <i>Virus</i>	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
65) <i>WAN</i>	<i>Wide Area Network</i> Rangkaian komputer untuk menyambungkan komputer dan peranti persisian yang terletak jauh di antara satu sama lain. Rangkaian kawasan luas memerlukan penggunaan modem.
66) <i>Warga JAS</i>	Personel kerajaan yang berkhidmat di JAS seluruh Malaysia samada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT JAS



- 
- | | |
|-------------------------|---|
| 67) <i>Wireless LAN</i> | Jaringan komputer yang terhubung tanpa wayar. |
| 68) <i>Worm</i> | Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri, yang biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini. |
| 69) Pentadbir ICT | adalah pegawai pentadbir sistem aplikasi, pegawai pentadbir pusat data dan keselamatan serta pegawai ICT di JAS Negeri. |

TUJUAN

1. Polisi Keselamatan Siber (PKS), Jabatan Alam Sekitar (JAS) ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

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

OBJEKTIF

3. Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti berikut:
 - (i) Menerangkan kepada semua pengguna merangkumi warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.
 - (ii) Memastikan keselamatan penyampaian perkhidmatan JAS di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi
 - (iii) Kerajaan, industri dan orang awam;

- 
- (iv) Memastikan kelancaran operasi JAS dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;
 - (v) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
 - (vi) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

PEMAKAIAN POLISI

- 4. Polisi ini terpakai kepada semua warga JAS dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

TADBIR URUS

5. Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS JAS, satu struktur tadbir urus iaitu Jawatankuasa Keselamatan ICT (JKICT) JAS telah diwujudkan seperti berikut:

Pengerusi : Pegawai Keselamatan ICT (ICTSO) JAS.

Ahli : Pengarah Bahagian Teknologi Maklumat;
Semua Ketua Seksyen dan Unit Bahagian Teknologi Maklumat; dan
Lain-lain ahli yang berkaitan.

Urus setia : Unit Operasi, Rangkaian & Pusat Data JAS (UORPD),
Bahagian Teknologi Maklumat, JAS

Bidang rujukan JKICT adalah seperti yang berikut:

Peranan dan tanggungjawab Jawatankuasa Keselamatan ICT (JKICT) kementerian adalah seperti berikut:

- (i) Merancang, melaksana, menyemak dan memantau dasar, strategi dan pelan tindakan operasi dan keselamatan ICT;
- (ii) Merancang, melaksana, menyelaraskan dan memantau pengurusan operasi dan keselamatan ICT;
- (iii) Merancang, melaksana, menyelaraskan dan memantau pelaksanaan dan operasi ICT; dan
- (iv) Melaporkan kemajuan, penyelarasan dan pemantauan keselamatan ICT kepada

JPICT.

ASET ICT

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

(i) Maklumat

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

(a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 28 Akta Rahsia Rasmi 1972.

(b) Maklumat Rasmi

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

(c) Maklumat Pengenalan Peribadi

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

(d) Data Terbuka

Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

(ii) Aliran Data

Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam JAS hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

- (a) Saluran komunikasi dan aliran data antara sistem di JAS;
- (b) Saluran komunikasi dan aliran data ke sistem luar; dan
- (c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.



(iii) Platform Aplikasi dan Perisian

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

(iv) Peranti Fizikal dan Sistem

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

- (a) Pelayan;
- (b) Peranti/Peralatan Rangkaian;
- (c) Komputer Peribadi/Komputer Riba;
- (d) Telefon/peranti pintar;
- (e) Media Storan;
- (f) Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
- (g) Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi Kerajaan; dan
- (h) Peranti pengesahan (*authentication devices*), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

(v) Sistem Luaran

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

(vi) Sumber Luaran

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

- (a) Perisian Sebagai Satu Perkhidmatan (SaaS)
- (b) Platform Sebagai Satu Perkhidmatan (Paas)
- (c) Infrastruktur Sebagai Satu Perkhidmatan (IaaS)
- (d) Storan Pengkomputeran Awan
- (e) Pemantauan Keselamatan
- (f) Perkhidmatan Pembangunan Sistem
- (g) Perkhidmatan Sewaan/ Perolehan Peralatan/Perisian ICT

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

RISIKO

7. JAS hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat.
Risiko ialah kebarangkalian JAS tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber JAS.
8. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber JAS.
9. Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

- (i) Kerentanan

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

- (ii) Ancaman

Mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

- (iii) Impak

Menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi JAS.

(iv) Tahap Risiko

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

(v) Penguraian Risiko

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

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

(1) Teknologi

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

(2) Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

(3) Manusia

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

(vi) Pengurusan Risiko

(a) Penyedia perkhidmatan digital di JAS hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:

- (1) mengenal pasti kerentanan;
- (2) mengenal pasti ancaman;
- (3) menilai risiko;
- (4) menentukan penguraian risiko;
- (5) memantau keberkesanan penguraian risiko; dan
- (6) memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

(b) Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** oleh Bahagian masing-masing dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu PKP JAS.

PRINSIP KESELAMATAN

10. Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori maklumat yang dikendalikan oleh sistem. Bagi mencapai objektif keselamatan maklumat, prinsip keselamatan berikut hendaklah dilaksanakan:

(i) Prinsip "Perlu-Tahu"

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

(ii) Hak Keistimewaan Minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

(iii) Pengasingan Tugas

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

(iv) Kawalan Capaian Berdasarkan Peranan

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

(v) Peminimuman Data

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

TEKNOLOGI

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

(i) Peringkat Pemprosesan Data

(a) Data-dalam-simpanan

(1) JAS hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-



langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

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

(b) Data-dalam-pergerakan

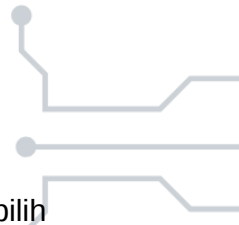
JAS hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

(c) Data-dalam-penggunaan

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

(d) Perlindungan Ketirisan Data

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

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

(ii) Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, JAS hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*countermeasure* dan *control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

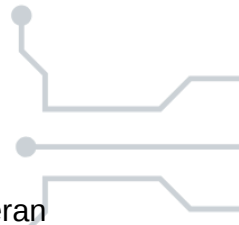
Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di JAS hendaklah digalakkan mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

(a) Peranti pengkomputeran peribadi

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

- (2) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon



kebenaran daripada JAS. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

(b) Peranti rangkaian

- (1) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan system seperti suis, penghala, tembok api, peranti VPN dan kabel.
- (2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(c) Aplikasi

- (1) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
- (2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data dalam simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(d) Pelayan

- (1) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
- (2) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(e) Persekitaran fizikal

- (1) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
- (2) JAS hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.
- (3) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.
- (4) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PROSES

11. Warga JAS hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

(i) Konfigurasi Asas

- (a) Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.
- (b) Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

(ii) Kawalan Perubahan Konfigurasi

- (a) Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
- (b) Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
- (c) Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

(iii) Sandaran

- (a) Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.
- (b) Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

(iv) Kitaran Pengurusan Aset

(a) Pindah

(1) Pemindahan hak milik aset berlaku dalam keadaan berikut;

- (a) Warga JAS meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;
- (b) Aset yang dikongsi untuk kegunaan sementara;
- (c) Pemberian aset kepada agensi lain; dan
- (d) Aset dikembalikan setelah tamat tempoh sewaan.

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

(b) Pelupusan

- (1) Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya

(2) Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

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

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

(c) Kitaran Hayat

(1) Kitaran hayat data hendaklah diuruskan mengikut Akta 629 - Akta Arkib Negara 2003

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

MANUSIA

12. Warga JAS, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

13. Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang

pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga JAS.

(i) Kompetensi Pengguna

(a) Kompetensi pengguna termasuk:

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

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

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

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

(ii) Kompetensi Pelaksana

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

(b) Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

(1) Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil professional keselamatan siber.

- 
- (2) Memenuhi keperluan pembelajaran berterusan.
 - (3) Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
 - (4) Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.
- (c) Pegawai Keselamatan ICT yang dilantik oleh JAS hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di JAS.

(iii) Peranan

- (a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
- (b) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.
- (c) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.
- (d) Warga JAS yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.
- (e) Warga JAS yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.

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

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

14. Setiap projek di JAS hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.
15. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), Polisi Keselamatan Siber JAS dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.
16. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, datadalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data.
17. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:
- (i) Peranti Pengkomputeran Peribadi
- (a) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.
- (b) Pengguna yang menggunakan peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi

yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

(ii) Peranti Rangkaian

- (a) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.
- (b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(iii) Aplikasi

- (a) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
- (b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(iv) Pelayan

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

(b) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(v) Persekitaran Fizikal

(a) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.

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

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

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

PERNYATAAN POLISI KESELAMATAN SIBER JAS

18. Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke

semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

19. Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(i) Kerahsiaan

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

(ii) Integriti

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

(iii) Tidak Boleh Disangkal

Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal

(iv) Kesahihan

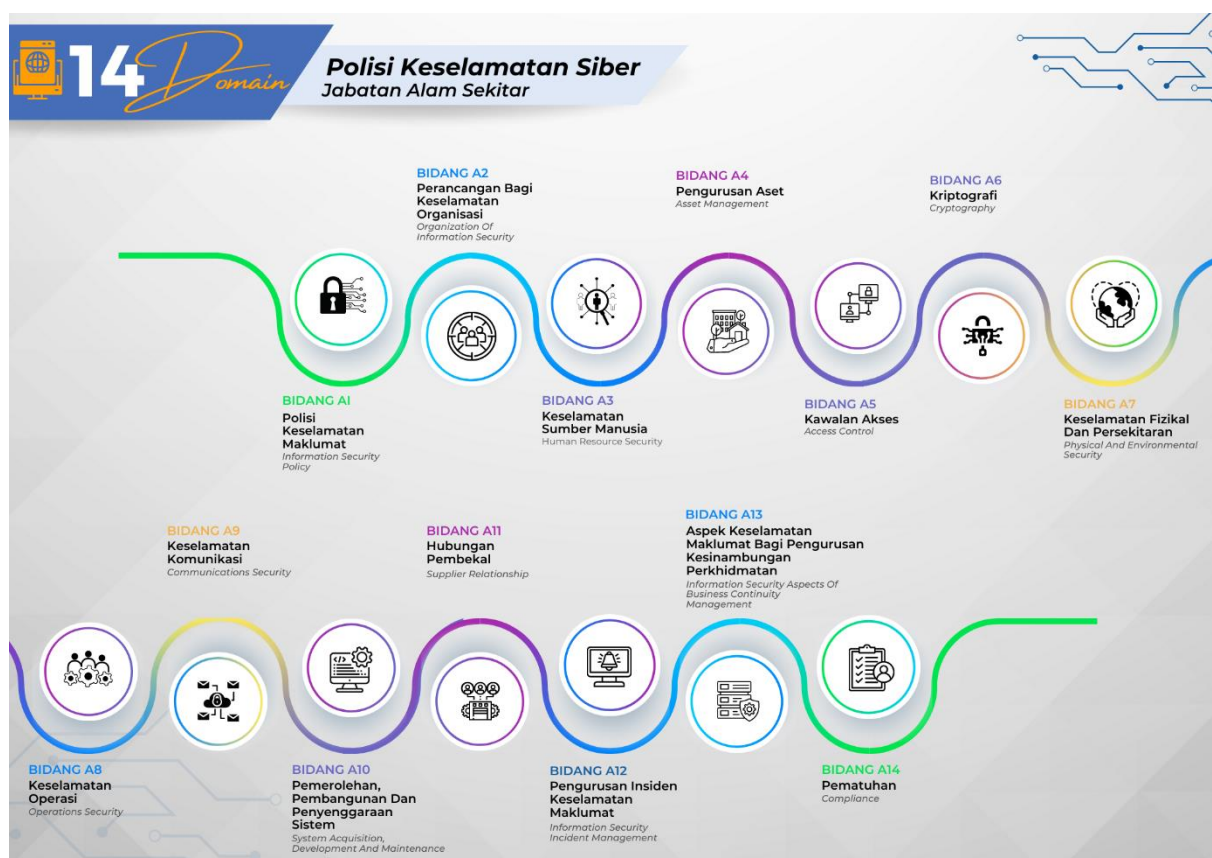
Data dan maklumat hendaklah dipastikan kesahihannya.

(v) Ketersediaan

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

20. Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT JAS, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

21. 14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber JAS diterangkan dengan lebih jelas dan teratur seperti berikut.



BIDANG A.1 : POLISI KESELAMATAN MAKLUMAT (*INFORMATION SECURITY POLICY*)

A.1.1 Hala Tuju Pengurusan Untuk Keselamatan Maklumat (*Management Directions for Information Security*)

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

A.1.1.1 Polisi Keselamatan Maklumat (*Policies for Information Security*)

Peranan: JPICT/CDO/ICTSO/ Pengarah Bahagian

Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah JAS dengan melalui Jawatankuasa Pemandu ICT yang terdiri daripada Timbalan Ketua Pengarah (Operasi), Timbalan Ketua Pengarah (Pembangunan), Pengarah Bahagian Teknologi Maklumat, Pegawai Keselamatan ICT, Pengarah-pengarah Bahagian dan ahli-ahli yang dilantik oleh Ketua Pengarah JAS.

Polisi Keselamatan Siber JAS mestilah dipatuhi oleh semua warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS.

Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan JAS kepada warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS.

A.1.1.2 Kajian Semula Polisi untuk Keselamatan Maklumat (*Review of Policies for Information Security*)

Peranan:JPICT/CDO/ICTSO

Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber JAS:

- (i) Mengenal pasti dan menentukan perubahan yang diperlukan;
- (ii) Mengemukakan cadangan pindaan kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT bagi tujuan pengesahan;
- (iii) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS; dan
- (iv) Polisi ini hendaklah dikaji semula setiap lima (5) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.

BIDANG A.2 : PERANCANGAN BAGI KESELAMATAN ORGANISASI (ORGANIZATION OF INFORMATION SECURITY)

A.2.1 Perancangan Dalaman (*Internal Organization*)

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber JAS.

A.2.1.1 Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and Responsibility of Information Security*)

(i) Ketua Pengarah

Peranan: Ketua Pengarah

Peranan dan tanggungjawab adalah seperti yang berikut:

- (a) Meluluskan penguatkuasaan pelaksanaan Polisi ini;
- (b) Memastikan warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;
- (c) Memastikan semua keperluan JAS seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi;
- (d) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan
- (e) Berperanan sebagai CDO atau melantik CDO dan ICTSO.

(ii) Ketua Pegawai Maklumat (CDO)

Peranan: CDO JAS

- (a) Peranan dan tanggungjawab CDO adalah seperti yang berikut:
- (b) Memantau pelaksanaan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan di dalam Polisi ini;
- (c) Memastikan kawalan keselamatan maklumat dalam JAS diseragam dan diselaraskan dengan sebaiknya; dan
- (d) Memastikan Pelan Strategik Pendigitalan JAS mengandungi aspek keselamatan siber.

(iii) Pegawai Keselamatan ICT (ICTSO)

Peranan: ICTSO

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:

- (a) Mewujudkan, prosedur selaras dengan keperluan Polisi ini;
- (b) Merangka pengurusan risiko dan audit keselamatan siber berpandukan peraturan kerajaan yang berkaitan dengan 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 CERT JAS dan seterusnya membantu dalam penyiasatan atau pemulihan;
 - (e) Melaporkan insiden keselamatan siber kepada CDO bagi insiden yang memerlukan kesinambungan perkhidmatan;
 - (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) Memastikan pelaksanaan pematuhan Polisi ini oleh warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS
 - (h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan
 - (i) Menyedia dan merangka latihan dan program kesedaran keselamatan siber.
 - (j) Menyelaras pelan latihan dan program kesedaran keselamatan siber.

(iv) Pengarah Bahagian dan Negeri

Peranan: Pengarah Bahagian dan Negeri

Peranan dan tanggungjawab Pengarah Bahagian dan Negeri ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut:

- (a) Penglibatan teknologi baru dan teknologi hijau bagi aplikasi yang berkaitan bahagian.

(b) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan;
dan

(c) Memastikan pematuhan kepada pelaksanaan peraturan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.

(v) Pentadbir ICT

Peranan: Pentadbir ICT

Peranan dan tanggungjawab Pentadbir ICT adalah seperti yang 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) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;

(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) Menyimpan dan menyemak rekod jejak audit; dan

(f) Bertanggungjawab memantau setiap perkakasan dan perisian ICT berada di dalam keadaan yang baik.

(vi) *Computer Emergency Response Team (CERT) JAS*

Peranan: CERT JAS

Peranan dan tanggungjawab CERT JAS adalah seperti yang berikut:

- (a) Menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden;
- (b) Merekod dan menjalankan siasatan awal insiden yang diterima;
- (c) Menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum;
- (d) Menasihati Pentadbir ICT untuk mengambil tindakan pemulihan dan pengukuhan; dan
- (e) Menyebar maklumat berkaitan pengukuhan keselamatan siber kepada Pentadbir ICT.

(vii) Pengguna

Peranan: Pengguna

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

- (a) Membaca, memahami dan mematuhi Polisi ini;
- (b) Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya;

- 
- (c) Menjalani tapisan keselamatan sekiranya berurusan dengan maklumat terperingkat;
 - (d) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan;
 - (e) Melaksanakan langkah-langkah perlindungan seperti yang berikut:
 - (1) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - (2) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - (3) Menentukan maklumat sedia untuk digunakan;
 - (4) Menjaga kerahsiaan maklumat;
 - (5) Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan;
 - (6) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - (7) Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.
 - (f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CERT JAS dengan segera;
 - (g) Menghadiri program-program kesedaran mengenai keselamatan siber; dan
 - (h) Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini.

A.2.1.2 Pengasingan Tugas (*Segregation of Duties*)

Peranan: Pengarah Bahagian dan Negeri

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;
- (ii) memastikan tugas mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan
- (iii) pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

A.2.1.3 Hubungan Dengan Pihak Berkuasa (*Contact with Authorities*)

Peranan: Bahagian Pentadbiran & Kewangan (BTW) JAS, Pasukan ERT, CERT JAS.

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- 
- (i) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab;
 - (ii) mewujudkan dan mengemas kini senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan
 - (iii) insiden keselamatan maklumat harus dilaporkan tepat masanya bagi mengurangkan impak insiden.

A.2.1.4 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus (*Contact with Special Interest Groups*)

Peranan: Warga JAS (Mengikut Bidang Kepakaran)

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menghadiri forum kumpulan berkepentingan khusus bagi:

- (i) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;
- (ii) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman
- (iii) keselamatan maklumat terkini;

- (iv) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
- (v) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

A.2.1.5 Keselamatan Maklumat dalam Pengurusan Projek (*Information Security in Project Management*)

Peranan: Warga JAS (Pasukan Projek)

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- i) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek JAS;
- ii) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
- iii) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;
- iv) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber JAS;
- v) Kontrak perlu mengandungi elemen keselamatan maklumat merangkumi keperluan kerahsiaan dan hak harta intelek; dan
- vi) penyediaan spesifikasi perolehan digalakkan memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.

A.2.2 Peranti mudah alih dan telekerja (*Mobile Devices and Teleworking*)

Objektif: Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

A.2.2.1 Polisi Peranti Mudah Alih (*Mobile Device Policy*)

(i) **Peranan:** BTM JAS

Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih.

(ii) **Peranan:** JPICT

Meluluskan dasar, arahan, peraturan dan langkah keselamatan berkaitan penggunaan peranti mudah alih ICT kepada warga JAS.

(iii) **Peranan:** Warga JAS

Perkara-perkara yang perlu dipatuhi:

- (a) pendaftaran ke atas peralatan mudah alih;
- (b) keperluan ke atas perlindungan secara fizikal;
- (c) kawalan ke atas pemasangan perisian peralatan mudah alih;
- (d) kawalan ke atas versi dan *patches* perisian;
- (e) sekatan ke atas akses perkhidmatan maklumat secara dalam talian;
- (f) perlu dilengkapi dengan perisian hasad; dan

- 
- (g) peralatan mudah alih hendaklah disimpan di tempat yang selamat apabila tidak digunakan.

A.2.2.2 Telekerja (*Teleworking*)

Peranan: Warga JAS

Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja

BIDANG A.3 : KESELAMATAN SUMBER MANUSIA (*HUMAN RESOURCE SECURITY*)

A.3.1 Sebelum Perkhidmatan (*Prior To Employment*)

Objektif: Memastikan warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

A.3.1.1 Tapisan Keselamatan (*Security Screening*)

Peranan:Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Tapisan keselamatan hendaklah dijalankan terhadap warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan
- (ii) menjalankan tapisan keselamatan untuk warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

A.3.1.2 Terma dan Syarat Perkhidmatan (*Terms and Conditions of Employment*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Persetujuan berkontrak dengan warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

- (i) menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS yang terlibat dalam menjamin keselamatan aset ICT; dan
- (ii) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

A.3.2 Dalam Tempoh Perkhidmatan (*During Deployment*)

Objektif: Memastikan warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

A.3.2.1 Tanggungjawab Pengurusan (*Management Responsibilities*)

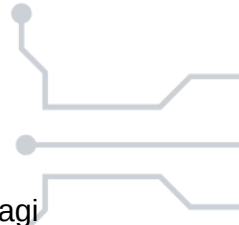
Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Pengurusan hendaklah memastikan warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.

A.3.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS.

- (i) Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:
- (ii) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber JAS dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;
- (iii) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber JAS perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

- 
- (iv) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

A.3.2.3 Proses Tatatertib (*Disciplinary Process*)

Pengguna: BTW (Sumber Manusia)

Proses tatatertib yang formal dan disampaikan kepada warga JAS hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga JAS yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga JAS sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh JAS;
- (ii) Warga JAS yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT JAS.

A.3.3 Penamatan dan Pertukaran Perkhidmatan (*Termination and Change of Employment*)

Objektif:Memastikan pertukaran, tamat perkhidmatan dan perubahan bidang tugas warga JAS diurus dengan teratur.

A.3.3.1 Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan (*Termination or Change of Employment Responsibilities*)

Peranan: BTM, BTW (Sumber Manusia) dan warga JAS

Warga JAS yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut:

- (i) Memastikan semua aset ICT dikembalikan kepada JAS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
- (ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JAS dan/atau terma perkhidmatan yang ditetapkan.
- (iii) Maklumat rasmi JAS dalam peranti tidak dibenarkan dibawa keluar dari JAS.

Warga JAS yang telah bertukar perkhidmatan hendaklah:

- (i) memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada JAS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
- (ii) menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.

BIDANG A.4 : PENGURUSAN ASET (*ASSET MANAGEMENT*)

A.4.1 Tanggungjawab Terhadap Aset (*Responsibility for Assets*)

Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JAS.

A.4.1.1 Inventori Aset (*Inventory of Assets*)

Peranan: Pegawai Penerima Aset, Pegawai Penyelaras Aset, Pegawai Aset dan warga JAS

Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT JAS.

Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:

- (i) JAS hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian/ Negeri untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT.
- (ii) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara, dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa.
- (iii) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.
- (iv) Pegawai Penyelaras Aset hendaklah mengesahkan penempatan aset ICT.

A.4.1.2 Pemilikan Aset (*Ownership of Assets*)

Peranan: Pegawai Aset, Pegawai Penyelaras Aset dan warga JAS

Aset yang diselenggara hendaklah hak milik JAS. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

- (i) memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;
- (ii) memastikan aset telah dikelaskan dan dilindungi;
- (iii) kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;
- (iv) memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan
- (v) memastikan semua jenis aset dipelihara dengan baik.

A.4.1.3 Penggunaan Aset yang Dibenarkan (*Acceptable Use of Assets*)

Peranan: Warga JAS

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

A.4.1.4 Pemulangan Aset (*Return of Assets*)

Peranan: BTW (Sumber Manusia), Pegawai Penyelaras Aset dan Warga JAS

Warga JAS hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.

A.4.2 Pengelasan Maklumat (*Information Classification*)

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

A.4.2.1 Pengelasan Maklumat (*Classification of Information*)

Peranan: Pegawai Pengelas

Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.

A.4.2.2 Pelabelan Maklumat (*Labelling of Information*)

Peranan: Warga JAS

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan Arahan Keselamatan.

A.4.2.3 Pengendalian Aset (*Handling of Assets*)

Peranan: Warga JAS

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampaikan, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:

- (i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- (ii) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa;
- (iii) Menentukan maklumat sedia untuk digunakan;
- (iv) Menjaga kerahsiaan kata laluan;
- (v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- (vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- (vii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.

A.4.3 Pengendalian Media (*Media Handling*)

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

A.4.3.1 Pengurusan Media Boleh Alih (*Management of Removal Media*)

Peranan: Pentadbir ICT dan Warga JAS

Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh JAS. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

- (i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
- (ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;
- (iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;
- (iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan
- (v) Menyimpan semua jenis media di tempat yang selamat.

A.4.3.2 Pelupusan Media (*Disposal of Media*)

Peranan: Pentadbir ICT dan Jawatankuasa yang dilantik untuk pelupusan aset.

- (i) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan.
- (ii) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.

A.4.3.3 Pemindahan Media Fizikal (*Physical Media Transfer*)

Peranan: Pentadbir ICT dan Jawatankuasa yang dilantik untuk pelupusan aset

- (i) Memastikan media yang mengandungi maklumat rasmi dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pengangkutan atau penghantaran.
- (ii) Sekiranya maklumat sulit pada media tidak dapat dibuat penyulitan (*encryption*), perlindungan fizikal tambahan pada media wajar dipertimbangkan

BIDANG A.5 : KAWALAN AKSES (*ACCESS CONTROL*)

A.5.1 Kawalan Akses (*Business Requirements of Access Control*)

Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

A.5.1.1 Polisi Kawalan Akses (*Access Control Policy*)

Peranan: Pemilik perkhidmatan digital dan Pentadbir ICT.

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza.

Kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini mengikut keperluan dan menyokong kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Keperluan keselamatan aplikasi;
- (ii) Hak akses berdasarkan klasifikasi maklumat;
- (iii) Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;
- (iv) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;
- (v) Pengasingan peranan kawalan capaian;
- (vi) Kebenaran rasmi permintaan akses;



(vii) Keperluan semakan hak akses berkala;

(viii) Pembatalan hak akses;

(ix) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan

(x) Capaian *privilege*.

A.5.1.2 Capaian kepada Rangkaian dan Perkhidmatan Rangkaian (*Access to Networks and Network Services*)

Peranan: ICTSO, Pengarah BTM dan Pentadbir Rangkaian

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

- (i) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian JAS, rangkaian agensi lain;
- (ii) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan
- (iii) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

A.5.2 Pengurusan Akses Pengguna (*User Access Management*)

Objektif: Akses 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.

A.5.2.1 Pendaftaran dan Pembatalan Pengguna (*User Registration and De-Registration*)

Peranan: Semua Pengguna dan warga JAS

Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi:

- (i) Akaun yang diperuntukkan oleh JAS sahaja boleh digunakan;
- (ii) Akaun pengguna mestilah unik;
- (iii) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada PYB (Pegawai Yang Bertanggungjawab) JAS terlebih dahulu;
- (iv) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
- (v) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan.

A.5.2.2 Peruntukan Akses Pengguna (*User Access Provisioning*)

Peranan: Pentadbir ICT

Proses pendaftaran dan pembatalan pengguna digunakan untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT.

A.5.2.3 Pengurusan Hak Akses Istimewa (*Management of Privileged Access Rights*)

Peranan: Pentadbir ICT

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.

Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

A.5.2.4 Pengurusan Maklumat Pengesahan Rahsia Pengguna (*Management of Secret Authentication Information of Users*)

Peranan: ICTSO dan Pentadbir ICT

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.

A.5.2.5 Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*)

Peranan: ICTSO dan Pentadbir ICT

Pemilik sistem dan Pentadbir ICT hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan.

Pentadbir ICT hendaklah menggunakan proses pendaftaran dan pembatalan pengguna untuk tujuan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

A.5.2.6 Pembatalan atau Pelarasan Hak Akses (*Removal or Adjustment of Access Rights*)

Peranan: Pentadbir ICT dan Pemilik Sistem

Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam JAS.

A.5.3 Tanggungjawab Pengguna (*User Responsibilities*)

Objektif:Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

A.5.3.1 Penggunaan Maklumat Pengesahan Rahsia (*Use of Secret Authentication Information*)

Peranan: Pengguna, Pentadbir ICT dan Pemilik Sistem

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

- (i) Membaca, memahami dan mematuhi Polisi Keselamatan Siber JAS;
- (ii) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;
- (iii) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat JAS;
- (iv) Melaksanakan langkah-langkah perlindungan seperti yang berikut:
 - (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

- 
- (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - (c) Menentukan maklumat sedia untuk digunakan;
 - (d) Menjaga kerahsiaan kata laluan;
 - (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
 - (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum.
 - (v) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO/ Pentadbir ICT dengan segera; dan
 - (vi) Menghadiri program-program kesedaran mengenai keselamatan siber.

A.5.3.2 Penggunaan Maklumat Pengesahan Rahsia (*Use of Secret Authentication Information*)

Peranan: Pengguna

Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.

A.5.4 Kawalan Akses Sistem dan Aplikasi (*System and Application Access Control*)

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.

A.5.4 Sekatan Akses Maklumat (*Information Access Restriction*)

Peranan: Pengguna, Pentadbir ICT

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut Polisi Kawalan Akses (merujuk kepada A.5.1.1)

A.5.5 Prosedur Log Masuk yang Selamat (*Secure Log-On Procedure*)

Peranan: Pentadbir ICT

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 yang berikut:

- (i) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan JAS;
- (ii) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;
- (iii) Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

- 
- (iv) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna;
 - (v) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti;
 - (vi) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

A.5.4.3 Sistem Pengurusan Kata Laluan (*Password Management System*)

Peranan: Pengguna, Pentadbir ICT, ICTSO

Sistem pengurusan kata laluan hendaklah interaktif dan mengambilkira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JAS seperti yang berikut:

- (i) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;
- (ii) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;
- (iii) Panjang kata laluan mestilah sekurang kurangnya **lapan (8) aksara** dengan gabungan huruf dan nombor
- (iv) Kata laluan hendaklah diingat dan tidak boleh_dicatat, disimpan atau didedahkan dengan apa cara sekali pun;
- (v) Kata laluan paparan kunci (*lock screen*) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;

- 
- (vi) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;
 - (vii) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;
 - (viii) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum TIGA (3) KALI sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan
 - (ix) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

A.5.4.4 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)

Peranan: Pentadbir ICT

Penggunaan program utiliti hendaklah dikawal bagi mengelakkan *Over-Riding* sistem.

A.5.4.5 Kawalan Akses Kepada Kod Sumber Program (*Access Control to Program Source Code*)

Peranan: Pentadbir ICT

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- (i) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;



(ii) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan

(iii) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik JAS.

BIDANG A.6 : KRIPTOGRAFI (*CRYPTOGRAPHY*)

A.6.1 Kawalan Kriptografi (*Cryptography Controls*)

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.

A.6.1.1 Polisi Penggunaan Kawalan Kriptografi (*Policy on The Use of Cryptographic Control*)

Peranan: CDO & ICTSO

Perkara-perkara berkaitan penyulitan maklumat yang perlu dipatuhi adalah seperti berikut:

- (i) Pengurusan maklumat terperingkat hendaklah dilaksanakan dengan menggunakan teknologi atau kaedah yang bersesuaian bagi melindungi maklumat terperingkat supaya tidak terdedah kepada mereka yang tidak sah.
- (ii) Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat terperingkat (rahsia dan rahsia besar) pada setiap masa.
- (iii) Mengenal pasti tahap perlindungan penggunaan penyulitan dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan.
- (iv) Maklumat terperingkat (rahsia dan rahsia besar) hendaklah melalui proses penyulitan setiap masa sebelum dihantar atau disalurkan ke dalam sistem rangkaian yang tidak selamat (seperti Internet, *mobile network* dan sebagainya).

A.6.1.2 Pengurusan Kunci Awam (*Public Key Management*)

Peranan: Warga JAS dan BTM

Pengurusan ke atas kekunci kriptografi hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kekunci daripada diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.

BIDANG A.7 : KESELAMATAN FIZIKAL DAN PERSEKITARAN (*PHYSICAL AND ENVIRONMENTAL SECURITY*)

A.7.1 Kawasan Selamat (*Secure Areas*)

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat JAS.

A.7.1.1 Perimeter Keselamatan Fizikal (*Physical Security Parameter*)

Peranan: Bahagian Pentadbiran dan Kewangan (BTW)

Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan Aset ICT JAS. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

- (i) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- (ii) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- (iii) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;
- (iv) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, rusuhan dan sebarang bencana alam atau perbuatan manusia;

- 
- (v) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;
 - (vi) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan
 - (vii) Memasang alat penggera atau kamera keselamatan;

A.7.1.2 Kawalan Kemasukan Fizikal (*Physical Entry Controls*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis JAS. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Setiap pegawai dan kakitangan JAS hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada BTW JAS apabila bertukar, tamat perkhidmatan atau bersara;
- (ii) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan
- (iii) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT JAS; dan
- (iv) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa.

A.7.1.3 Keselamatan Pejabat, Bilik dan Kemudahan (*Securing Offices, Rooms and Facilities*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;
- (ii) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan
- (iii) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.

A.7.1.4 Perlindungan Daripada Ancaman Luar Dan Persekitaran (*Protecting Against External and Environmental Threats*)

Peranan: Pentadbir Pusat Data dan BTW

Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. JAS perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, rusuhan dan bencana.

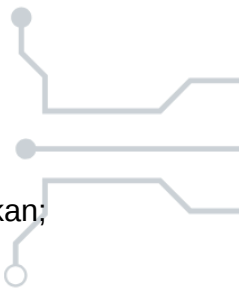
A.7.1.5 Bekerja di Kawasan Selamat (*Working in Secure Area*)

Peranan: Pentadbir Pusat Data dan BTW

Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga JAS yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis JAS termasuklah Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

- (i) Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik *server* atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;
- (ii) Akses adalah terhad kepada warga JAS yang telah diberi kuasa sahaja dan dipantau pada setiap masa;
- (iii) Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai;
- (iv) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;
- (v) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;
- (vi) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;
- (vii) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggaan, saluran air dan laluan awam;

- 
- (viii) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;
 - (ix) Memperkukuh dinding dan siling; dan
 - (x) Mengehadkan jalan keluar masuk.

A.7.1.6 Kawasan Penyerahan dan Pemunggahan (*Delivery and Loading Areas*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Titik kemasukan (*access point*) seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.

JAS hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

A.7.2 Peralatan ICT (*ICT Equipment*)

Objektif: Melindungi peralatan ICT JAS daripada kehilangan, kerosakan, kecurian dan disalahgunakan

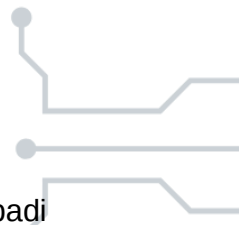
A.7.2.1 Penempatan dan Perlindungan Peralatan ICT (*Equipment Sitting and Protection*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

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 yang berikut:

- (i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;
- (ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
- (iii) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;
- (iv) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT;

- 
- (v) Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;
 - (vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;
 - (vii) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;
 - (viii) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Gen-Set);
 - (ix) Semua perkakasn hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan.
 - (x) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci;
 - (xi) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;
 - (xii) Peralatan ICT yang hendak dibawa ke luar premis JAS, perlulah mendapat kelulusan Pegawai Penyelaras Aset dan direkodkan bagi tujuan pemantauan;
 - (xiii) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut Pekeliling Perbendaharaan Pengurusan Aset Kerajaan ;

- 
- (xiv) Pengendalian Peralatan ICT hendaklah mamatuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;
 - (xv) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Pentadbir ICT;
 - (xvi) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir ICT untuk dibaik pulih;
 - (xvii) Sebarang pelekat selain bagi tujuan rasmi, hiasan, atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;
 - (xviii) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;
 - (xix) Pengguna dilarang sama sekali mengubah ***password administrator*** yang telah ditetapkan oleh pihak ICT; dan
 - (xx) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat yang bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan JAS sahaja.
 - (xxi) Sebarang pelaksanaan *rogue device* adalah dilarang.

A.7.2.2 Utiliti Sokongan (Supporting Utilities)

Peranan: Warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa.

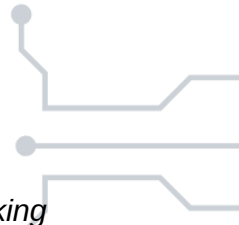
A.7.2.3 Keselamatan Kabel (*Cabling Security*)

Peranan: Pentadbir ICT

Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.

Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:

- (i) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- (ii) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;
- (iii) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

- 
- (iv) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.
 - (v) Menggunakan *port-based Network Access Control* atau PANA (*Protocol for Carrying Authentication for Network Access*) bagi sistem rangkaian kabel adalah sangat digalakan.

A.7.2.4 Penyelenggaraan Peralatan (*Equipment Maintenance*)

Peranan: Pegawai Penyelaras Aset, Pentadbir ICT

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

- (i) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;
- (ii) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
- (iii) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
- (iv) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

- 
- (v) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

A.7.2.5 Pengalihan Aset (*Removal of Assets*)

Peranan: Pengguna, Pegawai Penyelaras Aset

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

- (i) Peralatan ICT yang hendak dibawa keluar dari premis JAS untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Pengarah JAS atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan
- (ii) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.

A.7.2.6 Keselamatan Peralatan dan Aset di Luar Premis (*Security of Equipment Off-Premises*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis JAS. Peralatan yang dibawa keluar dari premis JAS adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- 
- (i) Peralatan perlu dilindungi dan dikawal sepanjang masa;
 - (ii) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan
 - (iii) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

A.7.2.7 Pelupusan yang Selamat atau Penggunaan Semula Peralatan (*Secure Disposal or Re-Use of Equipment*)

Peranan: Pegawai Penyelaras Aset, Pentadbir ICT dan warga JAS

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 JAS dan ditempatkan di JAS.

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 JAS. Langkah-langkah seperti yang berikut hendaklah diambil:

- (i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;
- (ii) Pegawai pemeriksa hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

- 
- (iii) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
 - (iv) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;
 - (v) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut:
 - (a) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.
 - (b) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM*, *Hardisk*, *Motherboard* dan sebagainya.
 - (c) Menyimpan dan memindahkan perkakasan luaran komputer seperti *AVR*, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di JAS.
 - (d) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan
 - (e) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab JAS.
 - (vi) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.
- 

- (vii) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; Sekiranya maklumat perlu disimpan, maka pentadbir ICT boleh membuat salinan;
- (viii) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan: Pelupusan yang berkuat kuasa;
- (ix) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan
- (x) Pegawai penyelaras aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem SPPA (Sistem Pemantauan Pengurusan Aset)

A.7.2.8 Peralatan Pengguna Tanpa Kawalan (*Unattended User Equipment*)

Peranan: Warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

- (i) Tamatkan sesi aktif apabila selesai tugas;
- (ii) *Log-off* komputer meja, komputer riba apabila sesi bertugas selesai; dan

- 
- (iii) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.

A.7.2.9 Dasar Meja Bersih dan Skrin Kosong (*Policy Clear Desk dan Clear Screen*)

Peranan: Warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Dasar meja bersih 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 atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuklah seperti yang berikut:

- (i) Menggunakan kemudahan *password screensaver* atau *logout* apabila meninggalkan komputer;
- (ii) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci;
- (iii) Memastikan semua dokumen diambil segera dari pencetak, pengimbas dan mesin fotostat.
- (iv) E-mel masuk dan keluar hendaklah dikawal; dan
- (v) Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.

BIDANG A.8 :KESELAMATAN OPERASI (*OPERATIONS SECURITY*)

A.8.1 Prosedur dan Tanggungjawab Operasi (*Operational Procedures and Responsibilities*)

Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.

A.8.1.1 Prosedur Operasi yang Didokumenkan (*Documented Operating Procedures*)

Peranan: Pengarah Bahagian dan Pentadbir ICT

Penyediaan dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

- (i) semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih digunakan hendaklah didokumenkan, disimpan dan dikawal;
- (ii) setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan
- (iii) semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan

A.8.1.2 Pengurusan Perubahan (*Change Management*)

Peranan: Pentadbir ICT

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:

- (i) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
- (ii) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
- (iii) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
- (iv) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.

A.8.1.3 Pengurusan Kapasiti (*Capacity Management*)

Peranan: Pemilik Sistem, Pentadbir ICT

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
- (ii) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

A.8.1.4 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (*Separation of Development, Test and Operational Environments*)

Peranan: Pentadbir ICT

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 yang berikut:

- (i) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*).

- 
- (ii) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan pembangunan; dan
 - (iii) Data yang mengandungi maklumat terperingkat tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

A.8.2 Perlindungan Daripada Perisian Hasad (*Protection from Malware*)

Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.

A.8.2.1 Kawalan Daripada Perisian Hasad (*Controls Against Malware*)

Peranan: Pentadbir ICT, Pengguna

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.

Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut:

- (a) Memasang sistem keselamatan untuk mengesan perisian atau program
- (b) *malware* seperti antivirus, dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

- 
- (c) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;
 - (d) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;
 - (e) Mengemas kini antivirus dengan *signature/pattern* antivirus yang terkini;
 - (f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
 - (g) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
 - (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.

A.8.3 Sandaran (Backup)

Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.

A.8.3.1 Sandaran Maklumat (*Information Backup*)

Peranan: Pentadbir ICT

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut polisi 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 lokasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
- (ii) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi;
- (iii) Menguji sistem sandaran sedia ada bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan
- (iv) Sandaran hendaklah dilaksanakan mengikut polisi yang dikonfigurasi. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.

A.8.4 Pengelogan dan Pemantauan (*Logging and Monitoring*)

Objektif: Merekodkan peristiwa dan menghasilkan bukti.

A.8.4.1 Pengelogan Kejadian (*Event Logging*)

Peranan: Pentadbir ICT

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat

seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.

Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data.

Jenis fail log bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:

- (i) Fail log sistem pengoperasian;
- (ii) Fail log servis (contoh: *web*, e-mel);
- (iii) Fail log aplikasi (audit trail); dan
- (iv) Fail log rangkaian (contoh: *switch*, *firewall*, *IPS*).

Pentadbir ICT hendaklah melaksanakan perkara-perkara berikut:

- (i) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
- (ii) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
- (iii) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti ketirisan maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada pasukan CERT JAS.

A.8.4.2 Perlindungan Maklumat Log (*Protection of Log Information*)

Peranan: Pentadbir ICT

Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

A.8.4.3 Log pentadbir dan Pengendali (*Administrator and Operator Logs*)

Peranan: Pentadbir ICT dan CERT JAS

Aktiviti pentadbir ICT dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap.

- (i) Memantau penggunaan kemudahan memproses maklumat secara berkala;
- (ii) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;
- (iii) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;
- (iv) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan
- (v) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti ketirisan maklumat dan pencerobohan, Pentadbir ICT hendaklah melaporkan kepada pasukan CERT JAS.

A.8.4.4 Penyegerakan Jam (*Clock Synchronisation*)

Peranan: Pegawai ICT

Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diselaraskan mengikut sumber rujukan masa tunggal.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JAS atau domain keselamatan perlu disegerakan dengan satu sumber waktu melalui *Network Time Protocol (NTP)* yang ditetapkan.

A.8.5 Kawalan Perisian yang Beroperasi (*Control of Operational Software*)

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

A.8.5.1 Pemasangan Perisian Pada Sistem yang Beroperasi (*Installation of Software on Operational Systems*)

Peranan: Pentadbir ICT

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:

- (i) Strategi *rollback* perlu dikenalpasti sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;

- 
- (ii) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan
 - (iii) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

A.8.6 Pengurusan Kerentanan Teknikal (*Technical Vulnerability Management*)

Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

A.8.6.1 Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)

Peranan: Pentadbir ICT dan CERT JAS

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 yang berikut:

- (i) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;
- (ii) Menganalisis tahap risiko kerentanan; dan

(iii) Mengambil tindakan pengolahan dan kawalan risiko.

A.8.6.2 Sekatan ke atas Pemasangan Perisian (*Restriction on Software Installation*)

Peranan: Pentadbir ICT, warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS.
- (ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; dan
- (iii) Mengimbas semua perisian atau sistem antivirus sebelum menggunakannya.

A.8.7 Pertimbangan Tentang Audit Sistem Maklumat (*Information Systems Audit Considerations*)

Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

A.8.7.1 Kawalan Audit Sistem Maklumat (*Information Systems Audit Controls*)

Peranan: ICTSO, dan Pentadbir ICT

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.

BIDANG A.9 : KESELAMATAN KOMUNIKASI (*COMMUNICATIONS SECURITY*)

A.9.1 Pengurusan Keselamatan Rangkaian (*Network Security Management*)

Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

A.9.1.1 Kawalan Rangkaian (*Network Control*)

Peranan: Pentadbir ICT

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;
- (ii) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir dan gegaran;
- (iii) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;
- (iv) *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;
- (v) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan JAS;

- (vi) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat JAS;
- (vii) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;
- (viii) Sebarang penyambungan rangkaian yang bukan di bawah kawalan BTM JAS adalah tidak dibenarkan;
- (ix) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di JAS sahaja dan penggunaan modem adalah dilarang sama sekali;
- (x) Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;
- (xi) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;
- (xii) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian JAS, rangkaian agensi lain dan rangkaian awam;
- (xiii) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;
- (xiv) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;
- (xv) Mengawal capaian fizikal dan logikal ke atas kemudahan *port* diagnostik dan konfigurasi jarak jauh;
- (xvi) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan JAS; dan

(xvii) Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan JAS.

A.9.1.2 Keselamatan Perkhidmatan Rangkaian (*Security of Network Services*)

Peranan: ICTSO, Pengarah Bahagian dan Negeri, Pentadbir ICT dan Pembekal

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.

A.9.1.3 Pengasingan Dalam Rangkaian (*Segregation in Networks*)

Peranan: ICTSO, Pengarah Bahagian dan Negeri dan Pentadbir ICT

Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian JAS.

A.9.2 Pemindahan Data dan Maklumat (*Information Transfer*)

Objektif: Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara JAS dan pihak luar terjamin.

A.9.2.1 Polisi dan Prosedur Pemindahan Data dan Maklumat (*Information Transfer Policies and Procedures*)

Peranan: Pengguna, warga JAS dan pembekal

Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;
- (ii) Terma pemindahan data, maklumat dan perisian antara JAS dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;
- (iii) Media yang mengandungi maklumat perlu dilindungi; dan
- (iv) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.

A.9.2.2 Perjanjian Mengenai Pemindahan Data dan Maklumat (*Agreements on Information Transfer*)

Peranan: CDO dan Pengarah Bahagian dan Negeri

JAS perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara JAS dengan pihak luar. Perkara yang perlu dipertimbangkan ialah:

- (i) Pengarah Bahagian dan Negeri hendaklah mengawal penghantaran dan penerimaan maklumat JAS;
- (ii) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat JAS;

- (iii) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan
- (iv) JAS hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

A.9.2.3 Pesanan Elektronik (*Electronic Messaging*)

Peranan: Warga JAS

Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti **LAMPIRAN A:**

- (i) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003;
- (ii) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet;
- (i) Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 – Langkah- langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan
- (ii) Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan

A.9.2.4 Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality Or Non-Disclosure Agreements*)

Peranan: ICTSO, Pengarah Bahagian, Pentadbir ICT, Pengguna dan Pembekal

Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan.

Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

BIDANG A.10 : PEMEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM (SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE)

A.10.1 Keperluan Keselamatan Sistem Maklumat (*Security Requirements of Information Systems*)

Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.

A.10.1.1 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (*Information Security Requirements Analysis And Specifications*)

Peranan: Pentadbir ICT

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:

- (i) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepian perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;
- (ii) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Keselamatan Siber JAS;

- 
- (iii) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan
 - (iv) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data.

A.10.1.2 Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam (*Securing Application Services on Public Networks*)

Peranan: Pentadbir ICT

Perkara yang perlu dipertimbangkan adalah seperti berikut:

- (i) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi JAS. Contoh perkhidmatan sumber luaran ialah:
 - (a) Perisian Sebagai Satu Perkhidmatan;
 - (b) Platform Sebagai Satu Perkhidmatan;
 - (c) Infrastruktur Sebagai Satu Perkhidmatan;
 - (d) Storan Pengkomputeran Awan; dan
 - (e) Pemantauan Keselamatan.
- (ii) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;
- (iii) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*);
- (iv) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;
- (v) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

- 
- (vi) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

A.10.1.3 Melindungi Transaksi Perkhidmatan Aplikasi (*Protecting Application Services Transactions*)

Peranan: ICTSO, Pengarah Bahagian dan Negeri dan Pentadbir ICT

Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- (i) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;
- (ii) Memastikan semua aspek transaksi dipatuhi:
 - (a) maklumat pengesahan pengguna adalah sah digunakan dan
 - (b) telah disahkan;
 - (c) mengekalkan kerahsiaan maklumat;
 - (d) mengekalkan privasi pihak yang terlibat; dan
 - (e) protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.
- (iii) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.

A.10.2 Keselamatan Dalam Proses Pembangunan dan Sokongan (*Security in Development and Support Services*)

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

A.10.2.1 Dasar Pembangunan Selamat (*Secure Development Policy*)

Peranan: ICTSO, Pengarah Bahagian dan Negeri dan Pentadbir ICT

Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- (i) Keselamatan persekitaran pembangunan;
- (ii) Keselamatan pangkalan data;
- (iii) Keperluan keselamatan dalam fasa reka bentuk;
- (iv) Keperluan *check point* keselamatan dalam carta perbatuan projek;
- (v) Keperluan pengetahuan ke atas keselamatan aplikasi;
- (vi) Keselamatan dalam kawalan versi; dan
- (vii) Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.

A.10.2.2 Prosedur Kawalan Perubahan Sistem (*System Change Control Procedures*)

Peranan: Pengarah Bahagian dan Negeri dan Pentadbir ICT

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;
- (ii) aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;
- (iii) mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan
- (iv) capaian kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada Pentadbir ICT yang dibenarkan sahaja.

A.10.2.3 Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi ***(Technical Review Of Applications After Operating Platform Changes)***

Peranan: Pentadbir ICT

Apabila platform operasi berubah, aplikasi penting jabatan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi.

Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform.
- (ii) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan
- (iii) Memastikan perubahan yang sesuai dibuat kepada PKP JAS dan Pelan Pemulihan Bencana Sistem yang berkaitan.

A.10.2.4 Sekatan Ke atas Perubahan Dalam Pakej Perisian *(Restrictions on Changes to Software Packages)*

Peranan: Pentadbir ICT, Pengarah Bahagian dan Negeri

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.

A.10.2.5 Prinsip Kejuruteraan Sistem Yang Selamat (*Secure System Engineering Principles*)

Peranan: Pentadbir ICT, Pengarah Bahagian dan Negeri

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat terjamin.

A.10.2.6 Persekitaran Pembangunan Selamat (*Secure Development Environment*)

Peranan: Pentadbir ICT dan Pengarah Bahagian dan Negeri

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

JAS perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:

- (i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;
- (ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;
- (iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;
- (iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; dan

- 
- (v) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.

A.10.2.7 Pembangunan oleh Khidmat Luaran (*Outsourced Software Development*)

Peranan: Pentadbir ICT, Pengarah Bahagian dan Negeri, ICTSO

JAS hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (*source code*) adalah menjadi **HAK MILIK** JAS. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Perkiraan perlesenan, kod sumber ialah **HAK MILIK** JAS dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource*;
- (ii) Keperluan kontrak untuk reka bentuk selamat, pengkodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;
- (iii) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;
- (iv) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.

A.10.2.8 Pengujian Keselamatan Sistem (*System Security Testing*)

Peranan: Pentadbir ICT, ICTSO

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem.

Perkara yang perlu dipatuhi adalah seperti yang berikut:



- 
- (i) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;
 - (ii) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan
 - (iii) menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.

A.10.2.9 Pengujian Penerimaan Sistem (*System Accepting Testing*)

Peranan: Pengguna, Pentadbir ICT, ICTSO

Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat (rujuk A.10.1.1 dan A.10.1.2) dan kepatuhan kepada Polisi Pembangunan Selamat (rujuk A.10.2.1);
- (ii) penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan
- (iii) pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan (*vulnerability scanner*).

A.10.3 Data Ujian (*Test Data*)

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.

A.10.3.1 Perlindungan Data Ujian (*Protection of Test Data*)

Peranan: Pengguna, Pentadbir ICT, ICTSO

Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;
- (ii) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;
- (iii) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan
- (iv) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.

BIDANG A.11 : HUBUNGAN PEMBEKAL (*SUPPLIER RELATIONSHIP*)

A.11.1 Keselamatan Maklumat Dalam Hubungan Pembekal (*Information Security in Supplier Relationships*)

Objektif: Memastikan aset ICT JAS yang boleh dicapai oleh pembekal dilindungi.

A.11.1.1 Polisi Keselamatan Maklumat Untuk Hubungan Pembekal (*Information Security Policy for Supplier Relationships*)

Peranan: Pengarah Bahagian dan Negeri, Pemilik Projek dan Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset JAS. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- (i) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;
- (ii) Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal;
- (iii) Mengawal dan memantau akses pembekal;
- (iv) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;
- (v) Jenis-jenis obligasi kepada pembekal;
- (vi) Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;

- 
- (vii) Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber JAS kepada pembekal;
 - (viii) Menandatangani **Surat Akuan Pematuhan Polisi Keselamatan Siber JAS (LAMPIRAN B)**; dan
 - (ix) Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.

A.11.1.2 Menangani Keselamatan Dalam Perjanjian Pembekal (*Addressing Security Within Supplier Agreements*)

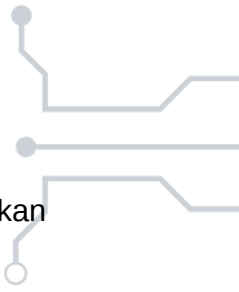
Peranan: Syarikat Pembekal

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak JAS selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) JAS hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;

- 
- (ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;
 - (iii) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;
 - (iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
 - (v) Jawatankuasa boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;
 - (vi) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut:
 - (a) Badan penilai pihak ketiga adalah bebas dan berintegriti;
 - (b) Badan penilai pihak ketiga adalah kompeten;
 - (c) Kriteria penilaian;
 - (d) Parameter pengujian; dan
 - (e) Andaian yang dibuat berkaitan dengan skop penilaian.
 - (viii) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JAS; dan

- 
- (ix) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JAS.

A.11.1.3 Rantaian Bekalan Teknologi Maklumat dan Komunikasi (*Information and Communication Technology Supply Chain*)

Peranan: Pengarah Bahagian dan Negeri, Pembekal dan Pemilik Projek

Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

- (i) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;
- (ii) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan
- (iii) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.

A.11.2 Pengurusan Penyampaian Perkhidmatan Pembekal (*Supplier Service Delivery Management*)

Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.

A.11.2.1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal (*Monitoring and Review Supplier Services*)

Peranan: Pengarah Bahagian dan Negeri, Pembekal dan Pemilik Projek

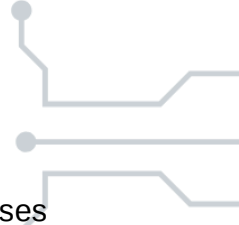
JAS hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

- (i) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal
- (ii) mematuhi perjanjian perkhidmatan;
- (iii) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan

A.11.2.2 Menguruskan Perubahan Kepada Perkhidmatan Pembekal (*Managing Changes to Supplier Services*)

Peranan: Pengarah Bahagian dan Negeri, Pembekal dan Pemilik Projek

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahankan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan,



hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut:

- (i) Perubahan dalam perjanjian dengan pembekal;
- (ii) Perubahan yang dilakukan oleh JAS bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan
- (iii) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, teknologi hijau, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.

BIDANG A.12 : PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT)

A.12.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan (Management of Information Security Incidents and Improvements)

Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.

A.12.1.1 Tanggungjawab dan Prosedur (*Responsibilities and Procedures*)

Peranan: ICTSO, Pengarah Bahagian, CERT JAS dan Pemilik Projek/Sistem Aplikasi

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden JAS adalah berdasarkan kepada Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut:

- (i) Memberikan kesedaran berkaitan Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT adan hebahan kepada warga JAS sekiranya ada perubahan; dan
- (ii) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

A.12.1.2 Pelaporan Kejadian Keselamatan Maklumat (*Reporting Information Security Events*)

Peranan: ICTSO, Pengarah Bahagian dan Negeri dan CERT JAS

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CERT JAS untuk tindakan seterusnya. ICTSO akan melaporkan kepada JPICT JAS dengan secara berkala. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (semak balik flow – Pelaporan insiden semasa kepada CERT. Cert Laporkan kpd JPICT secara berkala oleh ICTSO.)

- (i) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- (ii) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- (iii) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;
- (iv) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;
- (v) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan;
- (vi) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
- (vii) Berlaku percubaan mencerooboh, penyelewengan dan insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan siber berdasarkan:

- (i) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi;
- (ii) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan
- (iii) Prosedur Operasi Standard :Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT

A.12.1.3 Pelaporan Kelemahan Keselamatan Maklumat (*Reporting Security Weaknesses*)

Peranan: Warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Warga JAS dan pembekal yang menggunakan sistem dan perkhidmatan maklumat JAS dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.

A.12.1.4 Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat (*Assessment of and Decision on Information Security Events*)

Peranan: ICTSO

Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

A.12.1.5 Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Response to Information Security Incidents*)

Peranan: ICTSO, CERT JAS

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan **Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT**.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:

- (i) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;
- (ii) Menjalankan kajian forensik sekiranya perlu;
- (iii) Menghubungi pihak yang berkenaan dengan secepat mungkin;
- (iv) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;
- (v) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;
- (vi) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- (vii) Menyediakan tindakan pemulihan segera; dan
- (viii) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

A.12.1.6 Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning from Information Security Incidents*)

Peranan: ICTSO, CERT JAS

Pengetahuan yang diperoleh daripada penganalisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya.

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.

A.12.1.7 Pengumpulan Bahan Bukti (*Collection of Evidence*)

Peranan: ICTSO, CERT JAS

JAS hendaklah menentukan prosedur untuk mengenal pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.

BIDANG A.13 : ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (*INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT*)

A.13.1 Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan (*Management of Information Security Incidents and Improvements*)

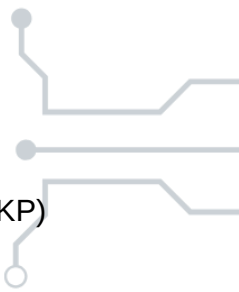
Objektif: Kesenambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes JAS.

A.13.1.1 Perancangan Kesenambungan Keselamatan Maklumat (*Planning Information Security Continuity*)

Peranan: Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan Bencana ICT

JAS hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, JAS perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi JAS.

JAS juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- 
- (i) Melantik pasukan tadbir urus Pengurusan Kesenambungan Perkhidmatan (PKP) JAS;
 - (ii) Menetapkan polisi PKP;
 - (iii) Mengenal pasti perkhidmatan kritikal;
 - (iv) Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis – BIA*) dan Penilaian Risiko terhadap perkhidmatan kritikal;
 - (v) Membangunkan Pelan Induk Pengurusan Kesenambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT.
 - (vi) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga JAS;
 - (vii) Melaksanakan simulasi dan penyelenggaraan berdasarkan BIA.

A.13.1.2 Pelaksanaan Kesenambungan Keselamatan Maklumat (*Implementing Information Security Continuity*)

Peranan: Koordinalor PKP, Pasukan Tindak balas Kesemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT

JAS hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluanlahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

- 
- (i) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal JAS yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesenambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;
 - (ii) Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP;
 - (iii) Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal JAS;
 - (iv) Mengemas kini struktur tadbir urus PKP JAS jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan
 - (v) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.

A.13.1.3 Menentusahkan, Mengkaji Semula dan Menilai Kesenambungan Keselamatan Maklumat (*Verify, Review and Evaluate Information Security Continuity*)

Peranan: Pengurusan Atasan JAS, Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT, Pemilik

Perkhidmatan Kritikal JAS dalam PKP dan warga JAS

JAS hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

A.13.2 Lewahan (*Redundancy*)

Objektif: Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

A.13.2.1 Ketersediaan Kemudahan Pemprosesan Maklumat (*Availability of Information Process Facilities*)

Peranan: Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir ICT

Kemudahan pemprosesan maklumat JAS perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.

BIDANG A.14 : PEMATUHAN (*COMPLIANCE*)

A.14.1 Pematuhan Terhadap Keperluan Perundangan dan Kontrak (*Compliance with Legal and Contractual Requirements*)

Objektif: Meningkatkan dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

A.14.1.1 Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai (*Identification of Applicable Legislation and Contractual Agreement*)

Peranan: Warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga JAS, pembekal dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JAS dan pembekal seperti

LAMPIRAN A.

A.14.1.2 Hak Harta Intelekt (*Intellectual Property Rights*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan



Intellectual Property Rights (IPR) dan juga pelesenan perisian. JAS akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat.

Perkara-perkara berikut hendaklah dipatuhi:

- (i) Pematuhan terhadap hak cipta yang berkaitan dengan perisian proprietari, dan reka bentuk yang diperoleh daripada JAS;
- (ii) Pematuhan terhadap perlesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh daripada JAS;
- (iii) Pematuhan terhadap hakcipta produk dan keperluan perlesenan; dan
- (iv) Pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.

A.14.1.3 Perlindungan Rekod (*Protection of Records*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

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.

A.14.1.4 Privasi dan Perlindungan Maklumat Peribadi (*Privacy and Protection of Personally Identifiable Information*)



Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

JAS hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

A.14.1.5 Kriptografi (*Regulation of Cryptographic Controls*)

Peranan: Warga JAS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JAS

A.14.2 Kajian Semula Keselamatan Maklumat (*Information Security Reviews*)

Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur JAS.

A.14.2.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)

Peranan: Pengarah Bahagian dan Negeri dan Pemilik Perkhidmatan

Penilaian keselamatan maklumat oleh pihak berkecuali hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

A.14.2.2 Pematuhan Polisi dan Standard Keselamatan (*Compliance with Security Policies and Standards*)

Peranan: Pengarah Bahagian dan Negeri dan Pemilik Perkhidmatan

JAS hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.

A.14.2.3 Kajian Semula Pematuhan Teknikal (*Technical Compliance Review*)

Peranan: Pengarah Bahagian dan Negeri dan Pemilik Perkhidmatan

JAS hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

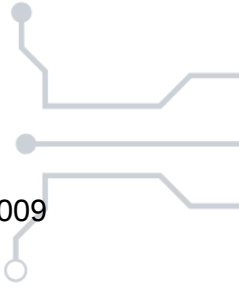
LAMPIRAN A

UNDANG-UNDANG DAN KONTRAK YANG TERPAKAI

Polisi ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut;

1. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";
2. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)*;
3. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
4. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis
5. Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan";
6. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
7. Surat Pekeliling Am Bil. 4 Tahun 2006 - "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";
8. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- "Tatacara Penyediaan, Penilaian dan Penerimaan Tender";

- 
9. Surat Pekeliling Perbendaharaan Bil. 3/1995 - "Peraturan Perolehan Perkhidmatan Perundingan";
 10. Akta Tandatangan Digital 1997;
 11. Akta Rahsia Rasmi 1972;
 12. Akta Jenayah Komputer 1997;
 13. Akta Hak Cipta (Pindaan) 2012;
 14. Akta Komunikasi dan Multimedia (Pindaan) 2004;
 15. Perintah-Perintah Am;
 16. Arahan Perbendaharaan;
 17. Arahan Teknologi Maklumat 2007;
 18. *Standard Operating Procedure (SOP) ICT JAS*;
 19. Etika Penggunaan E-mel dan Internet JAS;
 20. Surat Akujanji;
 21. Myportfolio;
 22. Pelan Kesyinambungan Perkhidmatan;
 23. Surat Arahan MAMPU.702-1/1/7 Jld. 3 (48) bertarikh 23 Mac 2009 bertajuk
 24. "Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-agensi Kerajaan";

- 
25. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 bertajuk "Penggunaan Media Jaringan Sosial di Sektor Awam";
 26. Pekeliling Perbendaharaan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan (TPA)";
 27. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001 :2013 Dalam Sektor Awam;
 28. Pekeliling Perkhidmatan Bil 5 2007 bertajuk "Panduan Pengurusan Pejabat bertarikh 30 April 2007";
 29. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT JAS;
 30. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016;
 31. Garis Panduan GPKI ; dan
 32. Surat Arahan Ketua Pengarah JAS bertarikh 1 Jun 2007 "Langkah-langkah mengenai penggunaan Mel Elektronik Agensi - Agensi Kerajaan", Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication (MyGovUC)*.



**SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER JAS**

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Jabatan :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

Tandatangan :

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

()

b.p. Ketua Pengarah Alam Sekitar

Tarikh: