



POLISI KESELAMATAN SIBER (PKS) VERSI 2.1

**LEMBAGA KEMAJUAN JOHOR TENGGARA (KEJORA)
KEMENTERIAN KEMAJUAN DESA DAN WILAYAH (KKDW)**

**DOKUMEN INI DAN SEGALA MAKLUMAT YANG TERKANDUNG DI DALAM DOKUMEN
INI ADALAH HAK MILIK KEJORA SEGALA BENTUK SALAHGUNA, SALINAN YANG
TIDAK MENDAPAT KEBENARAN DAN PENGELUARAN SEMULA DALAM SEMUA BENTUK
MEDIA ADALAH DILARANG.**

TERHAD



KEJORA

**POLISI KESELAMATAN SIBER (PKS)
LEMBAGA KEMAJUAN JOHOR TENGGARA (KEJORA)
VERSI 2.1**



REKOD PINDAAN DOKUMEN

No	Tarikh Pindaan	Versi	Butiran Pindaan
1.	26 April 2019	1.0	Keluaran Pertama
2.	27 April 2021	1.1	Penambahbaik A.6.2.2 Telekerja
3.	07 Ogos 2023	2.0	Penambahbaikan dokumen PKS KEJORA dengan mengambil kira standard ISO/IEC 27001:2022 yang Baharu.

ISI KANDUNGAN

POLISI KESELAMATAN SIBER (PKS)

KANDUNGAN	MUKA SURAT
1.0 PENGENALAN	1
1.1 OBJEKTIF	1
1.2 KANDUNGAN	1
1.3 PENYATAAN DASAR	2
1.4 SKOP	3
1.5 PRINSIP KESELAMATAN	6
1.6 PELANGGARAN DAN TINDAKAN DISIPLIN	8
1.7 SEMAKAN DAN PENYELENGGARAAN	8
2.0 TERMA DAN DEFINISI.....	9
2.1 RUJUKAN	9
2.2 TERMA DAN DEFINISI	9
3.0 PENILAIAN RISIKO KESELAMATAN ICT	16
4.0 TADBIR URUS KESELAMATAN ICT	17
5.0 KAWALAN ORGANISASI	22
6.0 KAWALAN MANUSIA.....	37
7.0 KAWALAN FIZIKAL	40
8.0 KAWALAN TEKNOLOGI.....	47
9.0 LAMPIRAN	60



1.0 PENGENALAN

1.0 PENGENALAN

Polisi Keselamatan Siber (PKS) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi dan Komunikasi Maklumat (ICT) Lembaga Kemajuan Johor Tenggara (KEJORA). PKS ini juga menerangkan kepada semua Pengguna ICT mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KEJORA.

1.1 OBJEKTIF

PKS KEJORA diwujudkan untuk memastikan tahap keselamatan ICT terus dan dilindungi bagi menjamin kesinambungan urusan KEJORA dengan meminimumkan kesan insiden keselamatan IT. Ianya dijadikan panduan kepada warga KEJORA dalam menguruskan dan melaksanakan aktiviti berkaitan ICT.

1.2 KANDUNGAN

PKS KEJORA mengandungi sembilan (9) bab utama seperti berikut:

1. BAB 1 – PENGENALAN
2. BAB 2 – TERMA DAN DEFINISI
3. BAB 3 – PENILAIAN RISIKO
4. BAB 4 – TADBIR URUS
5. BAB 5 – KAWALAN ORGANISASI
6. BAB 6 – KAWALAN MANUSIA
7. BAB 7 – KAWALAN FIZIKAL
8. BAB 8 – KAWALAN TEKNOLOGI
9. BAB 9 – LAMPIRAN

1.3 PENYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

1. Melindungi maklumat rahsia dan maklumat rasmi KEJORA daripada capaian oleh pihak yang tidak mempunyai kuasa yang sah;
2. Menjamin setiap maklumat adalah tepat dan sempurna;
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
4. Memastikan akses hanya kepada pengguna-pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

PKS KEJORA merangkumi perlindungan ke atas semua bentuk maklumat elektronik ataupun cetakan bagi bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua Pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

NO.	CIRI - CIRI	KETERANGAN
1.	Kerahsiaan	Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
2.	Integriti	Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.
3.	Tidak boleh disangkal	Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

4.	Kesahihan	Data dan maklumat hendaklah dijamin kesahihannya.
5.	Ketersediaan	Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

1.4 SKOP

Aset ICT KEJORA terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. PKS KEJORA menetapkan keperluan-keperluan asas keselamatan seperti berikut:

- Data dan maklumat termasuk *hardcopy* dan digital hendaklah diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan serta berkualiti; dan
- Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan KEJORA.

Bagi menentukan aset ICT di KEJORA sentiasa terjamin keselamatannya PKS KEJORA ini disediakan merangkumi perlindungan semua bentuk maklumat di KEJORA merangkumi proses pewujudan, pemusnahan, penyimpanan, penjanaan, percetakan, pengaksesan dan pengedaran. Ini akan dilakukan melalui pembangunan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:



a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan media storan digital di KEJORA. Contohnya komputer, pelayan, peralatan komunikasi dan sebagainya.

b) Perisian

Perisian aplikasi merangkumi semua program-program yang dipasang di setiap komputer dan server bagi tujuan pemprosesan data daripada pengguna. Contoh perisian aplikasi atau perisian sistem adalah sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KEJORA.

c) Perkhidmatan

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

- i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.
- ii. Sistem halangan akses seperti sistem "Door Access".
- iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain.

- iv. Perkhidmatan profesional seperti perunding , kepakaran teknikal dan latihan yang diberikan bagi memastikan kesinambungan pelaksanaan ICT di KEJORA.

d) Data atau Maklumat

Koleksi fakta dalam bentuk cetakan atau digital, yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif perkhidmatan KEJORA. Contohnya sistem dokumentasi, prosedur operasi, rekod KEJORA, maklumat pelanggan, pangkalan data/fail, maklumat arkib dan lain-lain.

e) Manusia

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

f) Premis Komputer Dan Komunikasi

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

Dasar ini adalah terpakai oleh semua pengguna di KEJORA sama ada anggota tetap, kontrak, pekerja sambilan, pelajar latihan industri, pembekal dan perunding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KEJORA.

1.5 PRINSIP KESELAMATAN

Prinsip-prinsip keselamatan yang menjadi asas kepada PKS KEJORA dan perlu dipatuhi adalah seperti berikut:



a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

b) Hak Akses Minimum

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlukan untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses akan dikemaskini dari masa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.



c) Akauntabiliti

Pengguna adalah bertanggungjawab keatas semua aset ICT, hak capaian dan tindakan yang telah diamanahkan.

d) Pengasingan

Tugas mewujudkan, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan dan dipantau oleh pihak tertentu bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi, perancangan dan perolehan.





e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti sebarang ketakakuran berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Justeru, pemeliharaan semua rekod yang berkaitan tindakan keselamatan adalah diperlukan. Aset-aset ICT seperti komputer, pelayan(server), router, firewall, Intrusion Prevention System (IPS), Antivirus dan peranti dan peralatan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit (audit trail).

f) Pematuhan

PKS KEJORA hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.



g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan ketersediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan berpunca dari insiden atau bencana. Pemulihan boleh dilakukan melalui aktiviti sandaran (backup) dan pewujudan pelan pemulihan bencana atau pelan kesinambungan perkhidmatan.

h) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum. KEJORA tidak boleh bergantung kepada satu individu, organisasi atau peralatan dalam pelaksanaan keselamatan ICT.



1.6 PELANGGARAN DAN TINDAKAN DISIPLIN

Sebarang pelanggaran terhadap PKS KEJORA perlulah dilaporkan pada ICT Security Officer (ICTSO). Setiap Insiden keselamatan perlu disiasat oleh ICTSO dengan kerjasama penyelia kakitangan terbabit dan pihak berkuasa yang berkaitan.

Pelanggaran polisi secara sengaja akan menyebabkan tindakan disiplin seperti:

- a) Kehilangan hak capaian ke atas sumber maklumat;
- b) Penilaian prestasi kerja yang buruk;
- c) Dikenakan tindakan tatatertib;
- d) Digantung kerja atau ditamatkan perkhidmatan;
- e) Ditamatkan kontrak; dan
- f) Dikenakan tindakan undang-undang.

1.7 SEMAKAN DAN PENYELENGGARAAN

ICT Security Officer (ICTSO) merupakan penulis dokumen PKS KEJORA ini. ICTSO bertanggungjawab untuk menyemak dan menyelenggara polisi ini sekurang – kurangnya setahun sekali bagi memastikan ianya sentiasa selari dengan penggunaan teknologi dan bersesuaian dengan perkhidmatan yang diberikan oleh KEJORA.

2.0 TERMA DAN SYARAT



2.0 TERMA DAN DEFINISI

2.0 TERMA DAN DEFINISI

2.1 RUJUKAN

BIL	DOKUMEN RUJUKAN
1.	<i>Malaysia Cyber Security Strategy, 2020 - 2024</i>
2.	Rangka Kerja Keselamatan Siber Sektor Awam, Versi 1.0, April 2016
3.	ISO/IEC 27001:2022 <i>Information security, cybersecurity and privacy protection – Information security controls</i>

2.2 TERMA DAN DEFINISI

BIL	TERMA	DEFINISI
1.	<i>Antivirus</i>	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM, <i>thumb drive</i> untuk sebarang kemungkinan adanya virus.
2.	Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
3.	Aset ICT	Peralatan ICT termasuk komputer, media storan, <i>server</i> , <i>router</i> , <i>firewall</i> , rangkaian dan lain-lain.
4.	<i>Backup</i>	Proses sandaran sesuatu dokumen atau maklumat.
5.	<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.

6.	BCP/PKP	<i>Business Continuity Planning/</i> Pelan Kesenambungan Perkhidmatan
7.	CCTV	<i>Closed-Circuit Television System</i> Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
8.	CSIRT Kementerian	<i>Computer Security Incident Response Team</i> Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
9.	CDO	<i>Chief Digital Officer</i> Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong misi dan visi organisasi.
10.	<i>Clear Desk dan 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.
11.	<i>Denial of service</i>	Halangan pemberian perkhidmatan.
12.	<i>Downloading</i>	Aktiviti muat turun sesuatu data.
13.	<i>Encryption</i>	Enkripsi atau penyulitan. Proses enkripsi data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
14.	<i>Firewall</i>	Sistem yang direkabentuk untuk menghalang capaian pengguna atau aliran trafik yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

15.	<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft / espionage</i>) dan penipuan (<i>hoaxes</i>).
16.	<i>Hard disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
17.	<i>Hub</i>	Hab (<i>hub</i>) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
18.	ICT	<i>Information and Communication Technology/</i> Teknologi Maklumat dan Komunikasi
19.	ICTSO	<i>ICT Security Officer</i> Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
20.	Insiden Keselamatan	Musibah (<i>adverse event</i>) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
21.	Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
22.	Intranet	Rangkaian dalaman yang dimiliki oleh sesebuah organisasi atau bahagian dan hanya boleh dicapai oleh kakitangan dan mereka yang diberi kebenaran sahaja.

23.	<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.
24.	<i>Intrusion Detection System (IDS)</i>	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 <i>host</i> atau rangkaian.
25.	<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.
26.	LAN	<i>Local Area Network</i> Rangkaian/ Kawasan Setempat yang menghubungkan peralatan IT.
27.	<i>Logout</i>	<i>Log-out</i> computer Keluar daripada sesuatu sistem atau aplikasi komputer.
28.	<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpakebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>Trojanhorse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.

29.	MODEM	MODulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
30.	<i>Outsource</i>	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
31.	Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau bahagian.
32.	<i>Public-Key Infrastructure (PKI)</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
33.	Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat KEJORA dan Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.
34.	Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada KEJORA dan Malaysia.
35.	<i>Restoration</i>	Pemulihan ke atas data, aplikasi dan infrastruktur ICT.

36.	<i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, capaian Internet.
37.	<i>Screen Saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
38.	<i>Server</i>	Komputer pelayan
39.	<i>Sulit</i>	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat KEJORA dan Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
40.	<i>Switches</i>	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian <i>Carrier Sense Multiple Access/Collision Detection (CSMA/CD)</i> yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
41.	<i>Terhad</i>	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
42.	<i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara yang bermotif personal dan atas sebab tertentu.

43.	<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.
44.	<i>Video Conference</i>	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
45.	<i>Video Streaming</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
46.	Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
47.	WAN	<i>Wide Area Network</i> Rangkaian yang merangkumi kawasan yang luas.
48.	Wireless LAN	Rangkaian komputer tanpa wayar.
49.	Worm	Sejenis virus yang boleh membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang tidak dilindungi atau tidak dikemaskini.



3.0 PENILAIAN RISIKO KESELAMATAN ICT

3.0 PENILAIAN RISIKO KESELAMATAN ICT

KEJORA hendaklah mengambil kira kewujudan risiko keselamatan ke atas aset ICT yang berpunca dari ancaman dan kerentanan yang semakin meningkat dan rumit. Justeru itu, KEJORA perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

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

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

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



4.0 TADBIR URUS KESELAMATAN ICT

4.0 TADBIR URUS KESELAMATAN ICT

Bagi memastikan keberkesanan PKS KEJORA, satu (1) struktur tadbir urus keselamatan ICT telah diwujudkan seperti berikut:

4.1 PENGURUSAN KEJORA

Keanggotaan Pengurusan KEJORA adalah sama dengan keanggotaan Mesyuarat Kajian Semua Pengurusan ISMS iaitu seperti berikut:

Pengerusi	Pengurus Besar / Timbalan Pengurus Besar (Pengurusan)
Ahli	1. Timbalan Pengurus Besar (Pembangunan) 2. Pengurus Bahagian 3. Ketua Unit
Urus setia	1. Pegawai Teknologi Maklumat 2. Penolong Pengurus di Bahagian Teknologi Maklumat

Peranan dan tanggungjawab Pengurusan KEJORA adalah seperti berikut:

- Meluluskan Polisi Keselamatan Siber KEJORA;
- Memperakui dan meluluskan Skop Persijilan ISMS;
- Memperakui penerimaan tahap risiko dan strategi perlindungan bagi menangani risiko aset ICT dalam skop ISMS yang ditahap "Medium" atau "High";
- Mesyuarat Kajian Semula Pengurusan ISMS (MKSP ISMS) untuk memantau dan menyemak pelaksanaan ISMS;
- Menetapkan arah tuju dan strategi untuk pelaksanaan ICT KEJORA;
- Merancang, mengenalpasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/strategi ICT KEJORA;
- Merancang dan menyelaraskan pelaksanaan program/projek ICT KEJORA supaya selaras dengan Pelan Strategik KEJORA;

- h) Menyelaras dan menyeragamkan pelaksanaan ICT antara KEJORA dengan Pelan Strategik ICT Sektor Awam;
- i) Mempromosi dan menggalakkan perkongsian pintar projek-projek ICT antara KEJORA;
- j) Merancang dan menentukan langkah-langkah keselamatan ICT;
- k) Memantau perkembangan program ICT KEJORA / serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT;
- l) Meluluskan perolehan ICT bagi KEJORA / berdasarkan had nilai projek perolehan KEJORA; dan
- m) Menyelaras dan memantau kemajuan pembangunan dan pelaksanaan projek ICT yang telah diluluskan.

4.2 PENGURUS BESAR

Peranan dan tanggungjawab Pengurus Besar KEJORA adalah seperti berikut:

- a) Memastikan penguatkuasaan pelaksanaan Polisi ini;
- b) Memastikan Kakitangan dan pengguna luar memahami dan mematuhi peruntukan - peruntukan di bawah Polisi ini;
- c) Memastikan semua keperluan KEJORA seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi;
- d) Memastikan pengurusan risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan
- e) Melantik CDO dan ICTSO.

4.3 KETUA PEGAWAI DIGITAL (CDO)

Peranan dan tanggungjawab CDO adalah seperti berikut:

- a) Membantu Pengurus Besar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT organisasi;
- b) Menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;
- c) Menentukan tindakan tata tertib yang perlu diambil ke atas pengguna yang telah dikenalpasti melanggar PKS;
- d) Mengkaji semula dan merumuskan tindakbalas pengurusan berdasarkan hasil penemuan audit dan menyediakan laporan berkaitan dengannya;

- e) Memastikan kawalan keselamatan maklumat dalam KEJORA diseragam dan diselaraskan dengan sebaiknya; dan
- f) Memastikan Pelan Strategik ICT KEJORA mengandungi aspek keselamatan ICT.

4.4 PEGAWAI KESELAMATAN ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) adalah merupakan Pengurus Teknologi Maklumat/ Pegawai Teknologi Maklumat Peranan dan tanggungjawab ICTSO adalah sebagaimana berikut:

- a) Mengurus keseluruhan program-program keselamatan ICT organisasi;
- b) Menguatkuasakan PKS organisasi;
- c) Memberi penerangan dan pendedahan berkenaan PKS KEJORA kepada semua pengguna;
- d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS;
- e) Menjalankan pengurusan risiko;
- f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti perisian hasad dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
- g) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT), KKDW dan memaklumkan kepada CDO;
- h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baikpulih dengan segera;
- i) Menyiasat dan mengenalpasti pengguna yang melanggar PKS KEJORA; dan
- j) Menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

4.5 PENTADBIR SISTEM ICT

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:

- a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam perkhidmatan tugas;
- b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan Ketua Pegawai Digital (CDO) sebagaimana yang telah ditetapkan di dalam PKS;
- c) Memantau aktiviti capaian harian pengguna;
- d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data yang berlaku tanpa kebenaran dan membatalkan atau memberhentikan aktiviti tersebut dengan serta merta;
- e) Menyimpan dan menganalisis rekod jejak audit;
- f) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala;
- g) Membaca, memahami dan mematuhi PKS;
- h) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan;
- i) Menentukan kawalan akses semua pengguna terhadap aset ICT;
- j) Melaporkan penemuan mengenai pelanggaran PKS kepada ICTSO; dan
- k) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT.

4.6 PENGGUNA ICT

Pengguna ICT merupakan sama ada anggota tetap, kontrak, pekerja sambilan, anggota MySTEP, pelajar latihan industri, pembekal dan perunding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KEJORA. Peranan dan tanggungjawab Pengguna ICT adalah sebagaimana berikut:

- a) Membaca, memahami dan mematuhi PKS organisasi;
- b) Mengetahui dan memahami implikasi keselamatan ICT;
- c) Lulus tapisan keselamatan;

- d) Melaksanakan prinsip-prinsip PKS dan menjaga kerahsiaan maklumat;
- e) Melaksanakan langkah-langkah perlindungan seperti berikut :-
 - i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
 - iii. Menentukan maklumat tersedia untuk digunakan;
 - iv. Menjaga kerahsiaan kata laluan;
 - v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
 - vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - vii. Menjaga kerahsiaan dan mengambil langkah-langkah keselamatan ICT dari diketahui umum.
- f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO atau Pegawai Teknologi Maklumat dengan segera;
- g) Menghadiri program kesedaran mengenai keselamatan ICT;
- h) Bertanggungjawab ke atas aset-aset ICT di bawah jagaannya; dan
- i) Menandatangani surat akuan pematuhan PKS.



5.0 KAWALAN ORGANISASI

5.0 KAWALAN ORGANISASI

Terdapat **Tiga puluh tujuh (37)** kawalan dalam Kawalan Organisasi iaitu sebagaimana berikut:

5.1 Polisi Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pelaksanaan polisi ini akan dijalankan dengan arahan Pengurus Besar KEJORA selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) KEJORA;
- b) PKS KEJORA perlu dihebahkan kepada semua Pengguna ICT yang menggunakan aset ICT dan ruang siber di KEJORA;
- c) PKS KEJORA perlu dipatuhi dan terpakai kepada semua Pengguna ICT. Tiada pengecualian bagi pematuhan PKS ini;
- d) PKS KEJORA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial; dan
- e) PKS KEJORA hendaklah dikaji semula dengan kekerapan sekurang-kurangnya **sekali setahun** atau mengikut keperluan.

5.2 Peranan dan Tanggungjawab Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengagihan peranan dan tanggungjawab keselamatan maklumat perlu dilakukan mengikut BAB 4 – Tadbir Urus Keselamatan ICT;
- b) Tanggungjawab untuk melindungi aset ICT dan untuk menjalankan proses keselamatan maklumat khusus perlu dikenalpasti; dan
- c) Tanggungjawab untuk aktiviti pengurusan risiko dan khususnya untuk penerimaan baki risiko hendaklah ditakrifkan.

5.3 Pengasingan Tugas

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; dan
- b) Tugas memadam, mengemas kini, dan mengubah data hendaklah mendapat kelulusan daripada pentadbir sistem atau ICTSO bagi mengelakkan capaian yang tidak dibenarkan serta melindungi aset ICT kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

5.4 Tanggungjawab Pengurusan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan Pengguna ICT diberi taklimat mengenai peranan dan tanggungjawab keselamatan maklumat mereka sebelum diberikan capaian kepada maklumat sulit atau sistem maklumat;
- b) Memastikan Pengguna ICT disediakan dengan garis panduan untuk menyatakan jangkaan keselamatan maklumat mengenai peranan mereka dalam KEJORA;
- c) Memastikan Pengguna ICT mencapai tahap kesedaran mengenai keselamatan maklumat yang berkaitan dengan peranan dan tanggungjawab mereka dalam KEJORA;
- d) Memastikan Pengguna ICT mematuhi terma dan syarat perkhidmatan, termasuk maklumat organisasi dasar keselamatan dan kaedah kerja yang sesuai; dan
- e) Memastikan Pengguna ICT disediakan saluran pelaporan untuk melaporkan pelanggaran polisi atau prosedur.

5.5 Hubungan Dengan Pihak Berkuasa

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mewujud dan mengemaskini senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan; dan
- b) Pihak yang dihubungi semasa kecemasan adalah termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal kuasa elektrik, keselamatan, kesihatan dan juga bomba.

5.6 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mewujud dan mengemaskini senarai kumpulan berkepentingan yang khusus; dan
- b) Menganggotai pertubuhan profesional ataupun forum pakar keselamatan maklumat bagi:
 - i. Meningkatkan ilmu pengetahuan berkaitan amalan terbaik dan perkembangan terkini mengenai keselamatan maklumat;
 - ii. Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat;
 - iii. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
 - iv. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

5.7 Perisikan Ancaman

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Maklumat yang berkaitan dengan ancaman keselamatan maklumat hendaklah dikumpulkan dan dianalisa untuk menghasilkan maklumat ancaman; dan
- b) Perisikan ancaman merangkumi lima (5) fasa seperti berikut:
 - i. Perancangan dan hala tuju;
 - ii. Pengumpulan data;
 - iii. Pemprosesan data;
 - iv. Menganalisis data; dan
 - v. Penyebaran dan maklum balas.

5.8 Keselamatan Maklumat dalam Pengurusan Projek

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;
- b) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan-kawalan yang diperlukan;
- c) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS KEJORA; dan
- d) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat.

5.9 Inventori Maklumat dan Aset Lain Yang Berkaitan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan semua aset dikendalikan oleh pengguna yang dibenarkan sahaja;
- b) Setiap pengguna ICT adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan
- c) Peraturan bagi pengendalian aset hendaklah dikenalpasti, didokumenkan dan dilaksanakan.

Prosedur berkaitan:

1. Prosedur Pengurusan Aset ICT (LKJT-ISMS-P2-008)

5.10 Penggunaan Maklumat dan Aset ICT Lain Berkaitan Yang Dibenarkan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengguna ICT mempunyai tanggungjawab untuk melaporkan dengan segera sebarang kejadian berkaitan keselamatan, kecurian, kehilangan, atau penggunaan Aset ICT yang tidak dibenarkan;
- b) Aset ICT hendaklah digunakan semata-mata untuk tujuan yang berkaitan dengan perkhidmatan KEJORA;
- c) Aset ICT tidak boleh dipindahkan, dan dipinjam untuk kegunaan peribadi;
- d) Pengguna ICT bertanggungjawab untuk membuat pertimbangan dan etika yang baik mengenai penggunaan peribadi Aset ICT;
- e) Pengguna ICT bertanggungjawab untuk melindungi semua data dan Aset ICT yang sensitif atau sulit di bawah pengawasan mereka;
- f) KEJORA mempunyai hak untuk memantau dan mengaudit semua Aset ICT pada bila-bila masa untuk tujuan keselamatan dan penyenggaraan; dan
- g) Pengguna ICT dikehendaki membaca PKS KEJORA ini dan menandatangani Surat Akuan Pematuhan PKS (Rujuk Lampiran 1).

Prosedur berkaitan:

1. Prosedur Pengurusan Aset ICT (LKJT-ISMS-P2-008)

5.11 Pemulangan Aset

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengguna ICT perlu memulangkan semua Aset ICT KEJORA yang berada di dalam jagaan mereka semasa penamatan perkhidmatan, kontrak atau perjanjian.
- b) Aset ICT berkenaan akan disimpan Bahagian Teknologi Maklumat untuk tujuan simpanan.

Prosedur berkaitan:

1. Prosedur Pengurusan Aset ICT (LKJT-ISMS-P2-008)

5.12 Pengelasan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Maklumat hendaklah dikelaskan sewajarnya berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada KEJORA; dan
- b) Memastikan setiap maklumat dikendalikan berdasarkan kepada tahap klasifikasi.

Prosedur berkaitan:

1. Prosedur Klasifikasi dan Pengendalian Maklumat (LKJT-ISMS-P2-001)

5.13 Pelabelan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Maklumat perlu dilabelkan sewajarnya mengikut skim klasifikasi maklumat yang digunakan oleh KEJORA.

Prosedur berkaitan:

1. Prosedur Klasifikasi dan Pengendalian Maklumat (LKJT-ISMS-P2-001)

5.14 Pemindahan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Maklumat yang akan dipindahkan kepada entiti luar perlu mendapat kelulusan pemilik maklumat.
- b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KEJORA dengan entiti luar.

Prosedur berkaitan:

1. Prosedur Pertukaran Maklumat (LKJT-ISMS-P2-004)

5.15 Kawalan Capaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengawal capaian ke atas maklumat, kemudahan pemprosesan maklumat dan proses perkhidmatan berdasarkan keperluan perkhidmatan dan keperluan keselamatan maklumat; dan

5.16 Pengurusan Identiti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kawalan perlu dilakukan ke atas peruntukan capaian dan proses pendaftaran pengguna baharu seperti kakitangan, pengguna luar dan pihak berkepentingan lain.
- b) Ini termasuklah proses pengesahan kebenaran sistem atau rangkaian untuk pengguna sedia ada dan proses pemansuhan ID pengguna yang tidak lagi diberi kuasa untuk mencapai sistem di KEJORA.

Prosedur berkaitan:

1. Prosedur Pengurusan ID Pengguna (LKJT-ISMS-P2-009)

5.17 Pengesahan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kata laluan tidak boleh dikodkan di dalam program dan ianya tidak boleh dipaparkan semasa proses pengesahan dibuat;
- b) Kata laluan awal yang unik mesti disediakan melalui kaedah yang selamat dan terkawal. Ianya perlu ditukar semasa proses log masuk yang pertama;
- c) Elakkan penggunaan kata laluan yang mudah diteka;
- d) Kata laluan asal yang dibekalkan oleh pihak pentadbir perlu ditukar apabila membuat pemasangan aplikasi, peranti, atau sistem operasi yang berkaitan;
- e) Tarikh luput kata laluan ditetapkan setiap tiga (3) bulan;
- f) Panjang minimum kata laluan ialah dua belas (12) aksara ; dan
- g) Kata laluan mestilah mengandungi kombinasi huruf, aksara khas dan angka.

Prosedur berkaitan:

1. Prosedur Pengurusan ID Pengguna (LKJT-ISMS-P2-009)

5.18 Hak Capaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Proses formal pendaftaran dan pemansuhan ID pengguna hendaklah dilaksanakan bagi membolehkan pemberian hak capaian;
- b) Proses formal peruntukan hak capaian pengguna hendaklah dilaksanakan dalam pemberian atau pemansuhan hak capaian kepada semua jenis pengguna untuk semua sistem dan perkhidmatan;
- c) Pemilik sistem atau aplikasi hendaklah mengkaji semula hak capaian pengguna pada jangka masa yang ditetapkan; dan
- d) Hak capaian semua kakitangan dan pengguna luar kepada maklumat dan kemudahan pemprosesan maklumat hendaklah dimansuhkan apabila ditamatkan penjawatan, kontrak atau perjanjian, atau diselaraskan apabila terdapat perubahan.

Prosedur berkaitan:

1. Prosedur Pengurusan ID Pengguna (LKJT-ISMS-P2-009)

5.19 Keselamatan Maklumat Dalam Hubungan Pembekal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; dan
- b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pembekal. Capaian kepada Aset ICT KEJORA perlu berlandaskan kepada kontrak perjanjian.

Prosedur berkaitan:

1. Prosedur Pengurusan Pembekal dan Pihak Ketiga (LKJT-ISMS-P2-012)

5.20 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan semua syarat keselamatan maklumat dinyatakan dengan jelas dalam perjanjian dengan pembekal.
- b) Menandatangani **Surat Akuan Pematuhan PKS KEJORA** seperti di **Lampiran 1**.

Prosedur berkaitan:

1. Prosedur Pengurusan Pembekal dan Pihak Ketiga (LKJT-ISMS-P2-012)

5.21 Pengurusan Keselamatan Maklumat Bagi Pembekalan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Perjanjian dengan pembekal haruslah merangkumi keperluan keselamatan untuk menangani sebarang risiko keselamatan maklumat yang berkaitan dengan ICT dan rantai bekalan produk/perkhidmatan.

Prosedur berkaitan:

1. Prosedur Pengurusan Pembekal dan Pihak Ketiga (LKJT-ISMS-P2-012)

5.22 Memantau, Mengkaji Semula dan Mengurus Perubahan Kepada Perkhidmatan Pembekal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam kontrak dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal;
- b) Memastikan perubahan dalam perkhidmatan pembekal dipersetujui bersama dan menguntungkan pihak KEJORA;
- c) Memastikan perubahan dalam perjanjian dengan pembekal mengambil kira maklumat kritikal KEJORA, sistem serta proses yang terlibat dan kajian risiko;
- d) Perubahan yang dilakukan oleh KEJORA bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan

- e) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi, produk, perkakasan yang baharu dan perubahan lokasi ataupun pertukaran pembekal.

Prosedur berkaitan:

1. Prosedur Pengurusan Pembekal dan Pihak Ketiga (LKJT-ISMS-P2-012)

5.23 Keselamatan Maklumat Bagi Penggunaan Perkomputeran Awan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Penilaian hendaklah dibuat secara terperinci berdasarkan kepada keperluan, pematuhan kepada dasar sedia ada dan kekangan undang-undang yang berkaitan sebelum sebarang keputusan untuk menggunakan perkhidmatan pengkomputeran awan dibuat;
- b) KEJORA hendaklah memastikan isi kandungan kontrak perjanjian seperti *Customer Agreement*, *Service Level Agreement* (SLA) atau *Acceptable Use Policy* (AUP) difahami sebelum mendaftar untuk menggunakan sebarang perkhidmatan;
- c) KEJORA boleh mempertimbangkan *Cloud Service Provider* (CSP) lain sekiranya sebarang terma di dalam kontrak tidak difahami dan meragukan;
- d) Data atau maklumat adalah hak milik eksklusif KEJORA sepenuhnya dan tidak boleh dianggap sebagai aset kepada CSP;
- e) KEJORA hendaklah diberikan hak untuk melaksanakan audit ke atas CSP untuk tujuan semakan seperti yang dinyatakan di dalam *Terms of Service* CSP; dan
- f) Klausula berhubung dengan pelucutan pentauliah (decommissioning) atau penamatan kontrak hendaklah dinyatakan dengan jelas di dalam kontrak perjanjian dengan CSP.

5.24 Perancangan dan Persediaan Pengurusan Insiden Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Prosedur pengurusan insiden keselamatan ICT perlu dilaksanakan berdasarkan Prosedur Pengurusan Insiden Keselamatan ICT.

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)

5.25 Penilaian dan Keputusan Mengenai Peristiwa Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Peristiwa keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)

5.26 Maklum Balas Kepada Insiden Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pegawai Keselamatan ICT (ICTSO) mesti memaklumkan status semasa insiden tersebut kepada pihak pengurusan; dan
- b) Komunikasi boleh dilakukan melalui salah satu daripada kaedah berikut:
 - i. Emel;
 - ii. Panggilan telefon;
 - iii. Secara terus;
 - iv. Media elektronik; atau
 - v. *Social Media Platform (whatsapp)*

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)

5.27 Belajar Daripada Insiden Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pegawai Keselamatan ICT (ICTSO) mesti mempunyai pengetahuan seiring dengan ancaman dan teknologi yang terkini; dan
- b) Mesyuarat harus diadakan dengan semua pihak yang terbabit selepas berlaku sesuatu insiden yang besar dan secara berkala bagi insiden-insiden yang kecil bagi tujuan:

- i. Analisis insiden;
- ii. Analisis punca insiden;
- iii. Tindakan pembetulan yang telah diambil dan keberkesanan
- iv. tindakan tersebut; dan
- v. Tindakan pencegahan yang mungkin untuk diambil bagi mengurangkan kebarangkalian pengulangan insiden.

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)

5.28 Pengumpulan Bukti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pegawai Keselamatan ICT (ICTSO) mesti mendokumenkan dengan jelas bagaimana bahan-bahan bukti termasuk sistem yang telah dikompromi akan dipelihara. Semua bahan bukti harus dikumpul mengikut prosedur yang menetapi undang-undang dan peraturan supaya boleh diterima pakai di mahkamah; dan
- b) Log yang terperinci mesti disimpan bagi setiap bahan bukti. Semua log mesti disenggara, disemak dan diawasi.

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)

5.29 Keselamatan Maklumat Semasa Gangguan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mewujudkan, mendokumenkan, melaksanakan dan menyenggarakan proses, prosedur dan kawalan bagi memastikan keperluan keselamatan maklumat dijaga semasa gangguan; dan
- b) Memastikan proses, prosedur dan kawalan tersebut disemak untuk keberkesanan.

Dokumen berkaitan:

1. Prosedur Pemulihan Bencana (LKJT-ISMS-P2-013)
2. Prosedur Pengurusan Penduaan dan Pemulihan (LKJT-ISMS-P2-014)

5.30 Kesiediaan ICT untuk Kesenambungan Perkhidmatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat sekiranya ianya dalam keadaan yang terjejas. Contohnya, semasa krisis atau bencana;
- b) Mewujudkan, mendokumenkan, melaksanakan dan menyelenggarakan proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan; dan
- c) Mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada jangka masa tertentu bagi memastikan ianya sah dan berkesan semasa keadaan yang menjejaskan.

5.31 Kenalpasti Keperluan Undang-Undang dan Kontrak Yang Terpakai

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan KEJORA perlu dinyatakan, didokumenkan, dan disimpan;
- b) Senarai perundangan dan peraturan yang berkuat kuasa dari masa ke semasa perlu dipatuhi oleh semua warga KEJORA adalah seperti di **Lampiran 2**.

5.32 Hak Harta Intelekt

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan penggunaan perisian yang sah;
- b) Memastikan pembelian dari sumber yang sah;
- c) Mengadakan program kesedaran terhadap dasar perlindungan harta intelek;
- d) Mengekalkan daftar aset dan mengenalpasti semua keperluan perlindungan terhadap aset;
- e) Menyimpan lesen perisian;
- f) Memastikan bilangan had lesen tidak melebihi had ditetapkan; dan

- g) Menjalankan pemeriksaan perisian yang sah dan produk berlesen digunakan.

5.33 Perlindungan Rekod

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Setiap rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pembebasan yang tidak dibenarkan, mengikut keperluan perundangan, peraturan, kontrak dan perkhidmatan; dan
- b) Penggunaan tandatangan digital hanya boleh digunakan untuk surat rasmi atau memo yang diklasifikasikan sebagai terbuka dan terhad sahaja.

Prosedur berkaitan:

1. Prosedur Kawalan Dokumen dan Rekod ISMS (LKJT-ISMS-P1-008)

5.34 Privasi dan Perlindungan Maklumat Peribadi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Perlindungan data peribadi perlu diwujudkan selaras dengan undang-undang sekiranya berkaitan.

5.35 Kajian Semula Keselamatan Maklumat Secara Bebas

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kajian semula secara berkala atau apabila perubahan ketara berlaku pada sebarang maklumat ICT KEJORA dan ia perlu dilakukan oleh pihak berkecuali atau pihak bebas.

5.36 Pematuhan Dasar dan Standard Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua Pengguna ICT di KEJORA perlu membaca, memahami dan mematuhi PKS KEJORA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa dari masa ke semasa;

- b) ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT; dan
- c) Pelanggaran PKS KEJORA boleh dikenakan tindakan tatatertib.

5.37 Prosedur Operasi Yang Didokumenkan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua prosedur keselamatan ICT yang diwujudkan, dikenal pasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal;
- b) Semua prosedur hendaklah dikemaskini dari masa ke semasa atau mengikut keperluan; dan
- c) Semua kakitangan KEJORA hendaklah mematuhi prosedur yang telah ditetapkan.

Prosedur berkaitan:

1. Prosedur Kawalan Dokumen dan Rekod ISMS (LKJT-ISMS-P1-008)





6.0 KAWALAN MANUSIA

6.0 KAWALAN MANUSIA

Terdapat **Lapan (8)** kawalan di bawah Kawalan Manusia iaitu seperti berikut:

6.1 Tapisan Keselamatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menjalankan tapisan keselamatan bagi setiap anggota baharu dan Pengguna ICT yang terlibat selaras dengan keperluan perkhidmatan; dan
- b) Pelaksanaan tapisan keselamatan menggunakan sistem e-Vetting yang disediakan oleh Majlis Keselamatan Negara (MKN).

6.2 Terma dan Syarat Perkhidmatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga KEJORA, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT KEJORA; dan
- b) Semua warga KEJORA yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.

6.3 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Setiap warga KEJORA perlu diberikan program kesedaran, pendidikan dan latihan tentang keselamatan ICT secara berterusan dalam melaksanakan tugas dan tanggungjawabnya;
- b) Program kesedaran, pendidikan dan latihan akan melibatkan semua pegawai KEJORA dan dilaksanakan secara berterusan;
- c) Laman web dan sosial media KEJORA akan dijadikan sebagai medium penyebaran maklumat berkaitan keselamatan ICT bagi meningkatkan tahap kesedaran pegawai KEJORA berkaitan kepentingan keselamatan ICT; dan

- d) Pegawai teknikal yang dipertanggungjawabkan menjaga keselamatan sumber ICT di mana ianya menyediakan perkhidmatan berpusat kepada pengguna (seperti *server, storage, switch, firewall, router, antivirus* berpusat dan lain-lain) akan dipastikan menjalani latihan yang spesifik berkaitan bidang tugas mengikut spesifikasi produk yang digunakan.

6.4 Proses Tatatertib

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas kakitangan KEJORA sekiranya berlaku pelanggaran dengan perundangan dan peraturan yang ditetapkan oleh KEJORA; dan
- b) Pelanggaran PKS KEJORA akan dikenakan tindakan tatatertib atau digantung dari mendapat akses kepada kemudahan ICT KEJORA.

6.5 Tanggungjawab Selepas Penamatan dan Pertukaran Perkhidmatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan semua aset ICT dikembalikan kepada KEJORA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan
- b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KEJORA dan/atau terma perkhidmatan.

6.6 Perjanjian Kerahsiaan dan Ketirisan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Keperluan bagi perjanjian kerahsiaan atau ketirisan maklumat yang mencerminkan keperluan KEJORA untuk melindungi maklumat perlu dikenalpasti, dikaji secara berkala jika perlu dan didokumenkan.

6.7 Telekerja atau Bekerja Dari Rumah

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan proses pengesahan pengguna *remote* digunakan untuk mengawal capaian logikal; dan
- b) Mengawal capaian logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh.

6.8 Pelaporan Peristiwa Keselamatan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Peristiwa Insiden keselamatan maklumat mesti dilaporkan kepada ICTSO dengan kadar segera; dan
- b) Insiden keselamatan maklumat adalah seperti berikut:
 - i. Maklumat disyaki atau didapati hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;
 - ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sistem maklumat digunakan tanpa kebenaran;
 - iii. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
 - iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
 - v. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini.

Prosedur berkaitan:

1. Prosedur Pengurusan Insiden Keselamatan ICT (LKJT-ISMS-P2-010)



7.0 KAWALAN FIZIKAL

7.0 KAWALAN FIZIKAL

Terdapat **Empat belas (14)** kawalan bagi Kawalan Fizikal iaitu seperti berikut:

7.1 Perimeter Keselamatan Fizikal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengenal pasti kawasan keselamatan fizikal dan lokasi keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset;
- b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;
- c) Menyediakan ruang menunggu khas untuk pelawat-pelawat;
- d) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan pegawai yang diberi kebenaran sahaja boleh melalui pintu masuk ini;
- e) Mengadakan kaunter kawalan;
- f) Memasang alat penggera, kamera litar tertutup (CCTV) dan seumpamanya; dan
- g) Mewujudkan perkhidmatan kawalan keselamatan.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.2 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Setiap warga KEJORA hendaklah memakai Pas Pekerja KEJORA sepanjang waktu bertugas;
- b) Pas Pekerja KEJORA hendaklah diserahkan balik kepada Bahagian Pentadbiran dan Pengurusan Sumber Manusia (PPSM) apabila pengguna berhenti, bertukar atau bersara;
- c) Setiap pelawat hendaklah mendapatkan Pas Pelawat dan hendaklah dipulangkan selepas tamat lawatan;

- d) Kehilangan pas mestilah dilaporkan dengan segera kepada Bahagian Pentadbiran dan Pengurusan Sumber Manusia (PPSM); dan
- e) Maklumat pelawat seperti tarikh, masa dan lokasi hendaklah direkod dan dikawal.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.3 Keselamatan Pejabat, Bilik dan Kemudahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab;
- b) Memasang alat penggera dan sistem CCTV;
- c) Sistem kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan
- d) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.4 Pemantauan Kawalan Fizikal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Reka bentuk sistem pemantauan harus dianggap sulit; dan
- b) Ujian yang kerap diperlukan untuk memastikan bahawa sistem pemantauan kawalan fizikal berfungsi.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.5 Perlindungan Daripada Ancaman Fizikal dan Persekitaran

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;
- b) Kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan alat pengesan asap;
- c) Peralatan perlindungan hendaklah dipasang di tempat yang sesuai, mudah dikenalpasti dan dikendalikan. Peralatan hendaklah disenggara dengan baik sekurang-kurangnya sekali setahun;
- d) Insiden persekitaran seperti kebakaran dan kebocoran air hendaklah dilaporkan segera kepada pihak yang bertanggungjawab;
- e) Untuk memastikan Bilik Server sentiasa selamat dari pencerobohan atau gangguan beberapa langkah boleh diambil seperti:
 - i. Semua server hendaklah diletakkan di Bilik Server atau bilik khas yang mempunyai sistem keselamatan yang baik. Pintu bilik hendaklah sentiasa tertutup dan berkunci;
 - ii. Sistem penghawa dingin hendaklah dihidupkan 24 jam sehari. Suhu persekitaran hendaklah berada di dalam lingkungan 20 hingga 27 darjah celsius dan kelembapan di paras 40% hingga 50%;
 - iii. Kesemua peralatan komputer di Bilik Server hendaklah dilengkapi dengan kemudahan UPS;
 - iv. Alat pemadam api hendaklah diletakkan di tempat yang mudah dilihat, tidak terhalang oleh sesuatu, mudah dicapai, tidak melepasi tarikh luput serta disenggara dengan baik;
 - v. Hanya pegawai atau pelawat yang dibenarkan boleh memasuki Bilik Server;
 - vi. Kontraktor/vendor dibenarkan memasuki Bilik Server dengan membuat imbasan kod QR yang disediakan; dan
 - vii. Setiap server hendaklah dilabelkan bagi memudahkan proses penyelenggaraan dilaksanakan.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.6 Bekerja di Kawasan Larangan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kawasan larangan ialah kawasan yang dihadkan kemasukan untuk pihak tertentu sahaja seperti Bilik Server, Bilik Fail dan Ruang Kerja yang menempatkan data dan maklumat sulit; dan
- b) Pihak ketiga dilarang memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah dipantau sepanjang masa sehingga tugas di kawasan berkenaan selesai.

Prosedur berkaitan:

1. Prosedur Pengurusan Keselamatan Fizikal Bilik Server dan Kawasan Larangan (LKJT-ISMS-P2-011)

7.7 Dasar Meja Bersih dan Skrin Kosong

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengaktifkan *screen lock* apabila meninggalkan komputer; dan
- b) Menyimpan maklumat terperingkat yang sensitif di dalam laci atau kabinet fail yang berkunci.

7.8 Penempatan dan Perlindungan Peralatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengguna bertanggungjawab sepenuhnya menjaga dan melindungi segala peralatan, komponen atau perkakasan ICT di bawah kawalannya agar sentiasa berkeadaan baik dan lengkap sepanjang masa;
- b) Setiap pengguna hendaklah memastikan semua peralatan ICT di bawah kawalannya disimpan di tempat yang bersih dan selamat;
- c) Pengguna dilarang memindah, menambah, membuang, atau menukar sebarang komponen atau peralatan ICT tanpa kebenaran BTM;
- d) Peminjaman dan pemulangan peralatan hendaklah direkodkan oleh pegawai yang telah dipertanggungjawabkan;
- e) Setiap pengguna adalah bertanggungjawab di atas kerosakan dan kehilangan peralatan ICT di bawah kawalannya; dan

- f) Setiap pengguna hendaklah melaporkan sebarang bentuk penyelewengan atau salah guna peralatan ICT kepada ICTSO.

7.9 Peralatan Dibawa Keluar Premis

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Peralatan ICT, maklumat atau perisian yang hendak dibawa keluar dari premis KEJORA perlu mendapat kelulusan daripada Pengurus BTM;
- b) Peralatan dan maklumat yang dibawa keluar dari pejabat hendaklah mendapat kelulusan pegawai berkaitan dan tertakluk kepada tujuan yang dibenarkan sahaja;
- c) Peralatan dan maklumat perlu dilindungi dan dikawal sepanjang masa;
- d) Memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan dan menyemak peralatan yang dipulangkan supaya berada dalam keadaan baik dan lengkap;
- e) Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih;
- f) Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kehilangan atau kerosakan;
- g) Peralatan mudah alih hendaklah disimpan atau dikunci di tempat yang selamat apabila tidak digunakan; dan
- h) memastikan peralatan mudah alih yang dibawa keluar dari pejabat perlu disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian.

7.10 Media Storan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Prosedur hendaklah dilaksanakan bagi pengurusan media storan menurut skim pengelasan maklumat yang diterima pakai;
- b) Media storan hendaklah dilupuskan dengan selamat melalui prosedur formal apabila tidak diperlukan lagi; dan
- c) Media storan yang mengandungi maklumat hendaklah dilindungi daripada capaian tanpa izin, penyalahgunaan atau kerosakan semasa proses pengangkutan.

Prosedur berkaitan:

7.11 Utiliti Sokongan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT;
- b) Menggunakan peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) bagi perkhidmatan kritikal seperti di Bilik Server dan Bahagian Kewangan; dan
- c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.

7.12 Keselamatan Kabel

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menggunakan kabel mengikut standard dan spesifikasi yang ditetapkan; dan
- b) Kabel dan laluan pemasangan kabel sentiasa dilindungi.

7.13 Penyelenggaraan Peralatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;
- b) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;
- c) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;
- d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;
- e) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

- f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus BTM/Pentadbir Sistem ICT; dan
- g) Penyelenggaraan peralatan ICT hanya boleh dilakukan oleh pegawai atau pihak yang dibenarkan sahaja.

Prosedur berkaitan:

1. Prosedur Pengurusan Aset ICT (LKJT-ISMS-P2-010)

7.14 Pelupusan Yang Selamat dan Penggunaan Semula Peralatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua kandungan peralatan khususnya maklumat rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat sandaran; dan
- b) Peralatan ICT yang akan dilupuskan sebelum dipindah milik dan hendaklah memastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.

Prosedur berkaitan:

1. Prosedur Pengurusan Aset ICT (LKJT-ISMS-P2-010)



8.0 KAWALAN TEKNOLOGI

8.0 KAWALAN TEKNOLOGI

Terdapat **Tiga puluh empat (34)** kawalan bagi Kawalan Teknologi iaitu seperti berikut:

8.1 Perkakasan Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pendaftaran ke atas perkakasan pengguna;
- b) Keperluan ke atas perlindungan secara fizikal;
- c) Kawalan ke atas pemasangan perisian;
- d) Kawalan ke atas versi dan *patches* perisian;
- e) Sekatan ke atas capaian perkhidmatan maklumat secara atas talian;
- f) Kawalan perkhidmatan maklumat secara kawalan capaian dan teknik kriptografi;
- g) Menyimpan di tempat yang selamat apabila tidak digunakan; dan
- h) Penggunaan telefon bimbit, peralatan komunikasi dan segala peralatan elektronik yang mampu merakam maklumat dalam mesyuarat yang membincangkan perkara Sulit, Rahsia dan Rahsia Besar KEJORA adalah dilarang.

8.2 Hak Capaian Istimewa

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pemberian dan penggunaan hak capaian istimewa kepada sistem atau maklumat KEJORA perlu dihadkan dan dikawal.

Prosedur berkaitan:

1. Prosedur Pengurusan ID Pengguna (LKJT-ISMS-P2-009)

8.3 Sekatan Capaian Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan dan dikawal mengikut keperluan.

Prosedur berkaitan:

1. Prosedur Pengurusan ID Pengguna (LKJT-ISMS-P2-009)

8.4 Capaian Kepada Kod Sumber

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; dan
- b) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.

8.5 Pengesahan Selamat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Mengawal capaian ke atas sistem dan aplikasi menggunakan prosedur log masuk yang terjamin;
- b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;
- c) Merekodkan capaian log masuk yang berjaya dan gagal;
- d) Notifikasi keselamatan jika ada potensi percubaan atau pencerobohan log masuk berjaya dikesan;
- e) Memaparkan maklumat tarikh dan masa log masuk dan setelah berjaya log masuk;
- f) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu;
- g) Tidak menghantar kata laluan dalam “clear-text” melalui rangkaian; dan
- h) Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.

8.6 Pengurusan Kapasiti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
- b) Penggunaan peralatan dan sistem mestilah dipantau dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti di masa akan datang untuk memastikan prestasi sistem berada di tahap optimum.

8.7 Perlindungan Daripada Perisian Hasad

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memasang perisian *antivirus* dan *Intrusion Prevention System (IPS)* bagi mengesan dan menghalang kemasukannya;
- b) Mengemas kini paten perisian *antivirus*;
- c) Menghadiri program kesedaran mengenai ancaman program merbahaya;
- d) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus;
- e) Memasukkan klausa tanggungan di dalam kontrak dengan pembekal perisian. Klausa bertujuan untuk tuntutan baik pulih sekiranya perisian mengandungi program merbahaya; dan
- f) Gunakan *antivirus* untuk mengimbas perisian sebelum menggunakannya bagi memastikan perisian bebas dari *virus*, *worm*, *Trojan* dan sebagainya.

Prosedur berkaitan:

1. Prosedur Perlindungan Daripada Kod Perosak (LKJT-ISMS-P2-002)

8.8 Pengurusan Kerentanan Teknikal

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memperoleh maklumat kerentanan teknikal yang tepat pada masanya ke atas sistem maklumat yang digunakan;
- b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan
- c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.

8.9 Pengurusan Konfigurasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan konfigurasi selamat mengikut keperluan keselamatan; dan
- b) Membuat sandaran kepada konfigurasi.

8.10 Penghapusan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Menghapuskan maklumat mengikut Arahan Keselamatan; dan
- b) Perlu mendapatkan kelulusan sebelum menghapuskan maklumat terperingkat.

8.11 Perlindungan Data (*Data Masking*)

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Melaksanakan perlindungan data terhadap data/maklumat yang digunakan untuk ujian pembangunan sistem; dan
- b) Perlindungan data melibatkan maklumat pengenalan peribadi.

8.12 Pencegahan Kebocoran Data

Pencegahan Kebocoran Data adalah proses kerja untuk mengesan dan menghalang sebarang pendedahan atau aktiviti pengekstrakan data tanpa kebenaran yang dilakukan oleh individu atau sistem. Langkah-langkah berikut perlulah dibuat bagi mencegah kebocoran data :

- a) Mengenalpasti dan mengklasifikasikan data / maklumat untuk dilindungi daripada kebocoran data;
- b) Memantau sumber / saluran kebocoran data / maklumat; dan
- c) Bertindak untuk menghalang data / maklumat daripada bocor.

8.13 Sandaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Sandaran daripada server atau komputer ke media storan lain perlu dilakukan dari masa ke semasa untuk mengelak kehilangan data sekiranya berlaku kerosakan *hard disk*;
- b) Kekerapan sandaran data bergantung kepada keperluan operasi dan kepentingan data tersebut sama ada secara harian, mingguan atau pun bulanan;
- c) Sandaran sistem aplikasi dan sistem pengoperasian perlu diadakan sekurang-kurangnya sekali bagi setiap versi;

- d) Sandaran yang melibatkan saiz data yang besar hendaklah dibuat di luar waktu bekerja untuk mengelakkan kesesakan rangkaian serta mengganggu prestasi server;
- e) Sandaran data yang penting dan kritikal dicadangkan dibuat satu (1) salinan dan disimpan di lokasi *offsite* yang berasingan bagi mengelakkan kemusnahan atau kerosakan fizikal disebabkan oleh bencana seperti kebakaran, banjir atau sebagainya;
- f) Sistem sandaran sedia ada hendaklah diuji bagi memastikan ianya dapat berfungsi, boleh dipercayai dan berkesan apabila digunakan (*restoration*) khususnya pada waktu kecemasan; dan
- g) Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam melakukan sandaran serta merancang penyalinan semula kepada media storan yang baru.

Prosedur berkaitan:

1. Prosedur Pengurusan Sandaran dan Pemulihan (LKJT-ISMS-P2-014)

8.14 Kelewahan (*redundancy*) Kemudahan Pemprosesan Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kemudahan pemprosesan maklumat perlu dilaksanakan dengan mewujudkan kelewahan (*redundancy*) yang mencukupi untuk memenuhi keperluan ketersediaan.

8.15 Pengelogan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap;
- b) Aktiviti pentadbiran dan operator sistem perlu direkodkan; dan
- c) Log hendaklah dilindungi dan pegawai yang dibenarkan sahaja boleh mengakses.

Prosedur berkaitan:

1. Prosedur Pengurusan Kawalan Log Keselamatan dan Log Masuk

8.16 Pemantauan Aktiviti

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memantau penggunaan kemudahan memproses maklumat secara berkala;
- b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari masa ke semasa dan menyediakan laporan jika perlu;
- c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;
- d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan
- e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO.

Prosedur berkaitan:

1. Prosedur Pengurusan Kawalan Log Masuk Keselamatan dan Log Masuk

8.17 Penyegerakan Jam

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KEJORA atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

8.18 Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Hanya program utiliti yang diperakui sahaja dibenarkan bagi kegunaan KEJORA; dan
- b) Penggunaan program atau perisian khas utiliti yang membebaskan kapasiti (*bandwidth*) rangkaian perlu dihadkan.

8.19 Pemasangan Perisian Pada Sistem Yang Sedang Beroperasi

Perisian yang sedang beroperasi perlu dikawal bagi memastikan integriti sistem dari sebarang kerentanan teknikal yang boleh di exploitasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Sebarang keperluan bagi menambah perisian yang baharu hendaklah dirujuk terlebih dahulu kepada pihak BTM atau Pengurusan KEJORA;
- b) Memastikan hanya perisian yang sah sahaja digunakan;
- c) Sebarang penambahbaikan atau menaiktaraf sebarang perisian perlu diuji di persekitaran pembangunan terlebih dahulu;
- d) Memastikan jejak log diaktifkan untuk proses penambahbaikan atau menaiktaraf perisian; dan
- e) Mengenal pasti strategi pemulihan sekiranya berlaku sebarang gangguan atau insiden semasa proses tambahbaik atau naiktaraf sesuatu perisian.

8.20 Kawalan Rangkaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan hak capaian ke atas sistem dapat dilaksanakan seperti yang ditetapkan;
- b) Sebarang cubaan mencerooboh dan aktiviti yang boleh mengancam sistem dan maklumat KEJORA perlu dipantau dan dikesan melalui pemasangan peralatan keselamatan seperti *Intrusion Prevention System (IPS)*;
- c) Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan KEJORA;
- d) Capaian ke atas kemudahan *port* diagnostik dan konfigurasi hendaklah dikawal;
- e) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance (SLA)* atau *Operational Level of Understanding (OLU)* yang telah ditetapkan;
- f) Penggunaan rangkaian tanpa wayar (*wireless*) LAN di KEJORA hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti Majlis Keselamatan Negara (MKN); dan

- g) Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer* atau *network analyzer* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO.

8.21 Keselamatan Perkhidmatan Rangkaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh, selamat dan bebas dari risiko seperti banjir, kilat, gegaran, habuk dan sebagainya;
- b) Ciri-ciri keselamatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenalpasti dan dinyatakan dalam perjanjian yang melibatkan perkhidmatan rangkaian;
- c) Konfigurasi peralatan rangkaian hendaklah mengaktifkan perkhidmatan atau nombor *port* yang diperlukan sahaja, mematikan penyiaran trafik (*network broadcast*), menggunakan kata laluan yang selamat, dan dilaksanakan oleh pegawai yang terlatih dan dibenarkan sahaja; dan
- d) Semua trafik rangkaian daripada dalam dan luar KEJORA dan sebaliknya mestilah melalui *firewall* dan hanya trafik yang disahkan sahaja dibenarkan untuk melepaskannya.

8.22 Pengasingan Dalam Rangkaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Membuat pengasingan rangkaian mengikut keperluan perkhidmatan; dan
- b) Mengasingkan capaian mengikut kumpulan perkhidmatan, maklumat pengguna dan sistem maklumat dalam rangkaian.

8.23 Saringan Capaian Web (*Web Filtering*)

- a) Mengenalpasti dan menyenarai hitam laman web berisiko; dan

- b) Mengenalpasti kaedah yang berkesan dan sesuai digunakan bagi menghalang atau menyaring capaian pengguna ke laman web tersebut.

8.24 Penggunaan Kriptografi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua maklumat yang terperingkat perlu disulitkan (*encrypt*) sebelum dihantar keluar. Pengguna boleh melaksanakan proses penyulitan dengan menggunakan sekurang-kurangnya kata laluan pada dokumen yang perlu dihantar;
- b) Media storan yang menyimpan maklumat terperingkat seperti *external harddisk* dan sebagainya perlu dilaksanakan penetapan kata laluan bagi mengelakkan pencerobohan maklumat;
- c) Komputer riba yang menyimpan maklumat terperingkat perlu dilaksanakan penetapan kata laluan yang kukuh terutamanya jika berada di luar premis bagi mengelakkan pencerobohan maklumat;
- d) Kata laluan perlu ditukar sekiranya berlaku kebocoran dan penyalahgunaan;
- e) Capaian secara *remote* perlu menggunakan kaedah yang selamat; dan
- f) Penggunaan *Secure Socket Layer* (SSL) adalah diwajibkan bagi semua sistem berasaskan web yang membenarkan pertukaran maklumat.

8.25 Kitaran Hayat Pembangunan Yang Selamat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Panduan keselamatan dalam kitar hayat pembangunan (*development life cycle*) perisian;
- b) Keselamatan repositori dengan mewujudkan repositori yang selamat untuk perisian/sistem maklumat yang dibangunkan;
- c) Kawalan keselamatan bagi versi kod sumber;
- d) Keperluan pengetahuan keselamatan dalam pembangunan perisian dengan membina kemahiran pembangun perisian/ sistem maklumat supaya mampu menjauhi, mengenal pasti, dan merungkai setiap kelemahan yang dikesan dalam perisian/ sistem maklumat yang dibangunkan. Teknik pengaturcaraan selamat wajar dipraktik;

- e) Kod sumber perlu selamat dan bebas daripada sebarang ancaman pencerobohan; dan
- f) Jika pembangunan perisian dilaksanakan dengan menggunakan sumber luar, KEJORA perlu mendapatkan jaminan bahawa pembekal yang dilantik memenuhi peraturan, polisi, prosedur dan proses berkaitan pembangunan sistem selamat.

8.26 Keperluan Keselamatan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Perolehan, pembangunan, penambahbaikan dan penyenggaraan aplikasi hendaklah mengambil kira kawalan keselamatan;
- b) Semua aplikasi yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa;
- c) Semua aplikasi yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; dan
- d) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan.

8.27 Seni Bina dan Prinsip Kejuruteraan Sistem Selamat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Memastikan keselamatan seperti ancaman daripada bencana alam dan manusia diambil kira;
- b) Perlindungan maklumat dalam pembangunan sistem semasa pemprosesan, perpindahan dan penyimpanan; dan
- c) Mengambil kira kriteria di bawah dalam prinsip kejuruteraan pembangunan sistem:
 - i. **Business Layer** – berdasarkan tahap pengesahan pengguna; hanya pengguna tertentu boleh melihat data peribadi;

- ii. **Data Layer** – hanya log masuk dengan kata laluan pangkalan data yang selamat untuk aktiviti penyenggaraan pangkalan data dibenarkan;
- iii. **Application Layer** – penggunaan enkripsi untuk penghantaran maklumat; dan
- iv. **Technology Layer** – penggunaan perisian sumber terbuka dan infrastruktur rangkaian.

8.28 Pengekodan Selamat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Kaedah pengkodan yang selamat perlu sentiasa dipraktiskan dengan memasukkannya sebagai salah satu keperluan dalam setiap fasa pembangunan aplikasi.
- b) Amalan pengkodan selamat boleh mengelakkan dari risiko rentanan aplikasi yang menjurus kepada ketirisan maklumat sensitif.

8.29 Ujian Keselamatan dan Penerimaan Dalam Pembangunan Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Ujian keselamatan sistem hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan *sistem output* untuk memastikan data yang telah diproses adalah tepat;
- b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum ianya digunakan;
- c) Kriteria penerimaan untuk peralatan dan sistem baharu, peningkatan dan versi baharu perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan
- d) Semua sistem baharu (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

8.30 Pembangunan Sistem oleh Sumber Luaran

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Semua pembekal yang melaksanakan kerja *outsourcing* dimestikan lulus dan melepasi tapisan keselamatan;
- b) Maklumat berperingkat hendaklah dimaklumkan secara *need to know basis*;
- c) Antara butir-butir yang perlu dinyatakan di dalam kontrak *outsourcing* adalah:
 - i. Kesahihan dan kerahsiaan logikal organisasi mesti dipelihara;
 - ii. Pegawai KEJORA mesti membuat pengujian terhadap sistem yang dibangunkan; dan
 - iii. Mesti menyatakan faktor keselamatan secara terperinci pada *Schedule Of Compliance (SOC)*.
- d) Pemindahan teknologi atau *Transfer Of Technology (TOT)* mesti dilaksanakan oleh pembekal kepada pengguna; dan
- e) Capaian secara fizikal dan logikal mesti dipantau oleh pegawai KEJORA yang dilantik bagi menguruskannya.

8.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan di persekitaran produksi; dan
- b) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

8.32 Pengurusan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Pengubahsuaian mestilah mendapat kebenaran pihak pengurusan atau pemilik aset ICT terlebih dahulu;

- b) Aktiviti-aktiviti seperti pemasangan, penyelenggaraan, mengemas kini komponen aset dan sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan dan kemahiran atau terlibat secara langsung dengan aset ICT berkenaan; dan
- c) Aktiviti perubahan atau pengubahsuaian hendaklah mematuhi spesifikasi atau kriteria yang ditetapkan dan hendaklah direkodkan serta dikawal bagi mengelakkan berlakunya ralat.

Prosedur berkaitan:

1. Prosedur Pengurusan Perubahan ICT (LKJT-ISMS-P2-015)

8.33 Perlindungan Maklumat Data Ujian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal;
- b) *Data input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian;
- c) Menggunakan kaedah perlindungan data (*data masking*) sekiranya perlu;
- d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian; dan
- e) *Data output* daripada aplikasi perlu disahkan bagi memastikan data yang dihasilkan adalah tepat.

8.34 Perlindungan daripada Audit dan Ujian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

- a) Keperluan audit dan ujian ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.
- b) Capaian ke atas peralatan sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.



9.0 LAMPIRAN

9.0 LAMPIRAN

9.1 Lampiran 1(a) – Surat Akuan Pematuhan PKS KEJORA (Anggota)



SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KEJORA

Nama (Huruf Besar) :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan PKS KEJORA serta apa-apa peraturan dan arahan lain yang berkaitan dikeluarkan dan dikuatkuasakan dari masa ke semasa selanjutnya tempoh perkhidmatan saya;
2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam PKS KEJORA; dan
3. Sekiranya saya didapati melanggar dasar yang telah ditetapkan, maka saya bersetuju dengan tindakan undang-undang yang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan :

Tarikh :

Disahkan Oleh:
Pegawai Keselamatan ICT (ICTSO)

(.....)

Tarikh:

Polisi Keselamatan Siber (PKS) boleh dicapai menerusi

<https://www.kejora.gov.my>.

9.2 Lampiran 1(b) – Surat Akuan Pematuhan PKS KEJORA (Syarikat)



SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER KEJORA (SYARIKAT)

Nama Syarikat :

No. Pendaftaran Syarikat :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan PKS KEJORA serta apa-apa peraturan dan arahan lain yang berkaitan dikeluarkan dan dikuatkuasakan dari masa ke semasa selanjutnya tempoh perkhidmatan saya;
2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam PKS KEJORA; dan
3. Sekiranya saya didapati melanggar dasar yang telah ditetapkan, maka saya bersetuju dengan tindakan undang-undang yang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

Tandatangan :

Tarikh :

Disahkan Oleh:
Pegawai Keselamatan ICT (ICTSO)

.....
()

Tarikh:

9.3 Lampiran 2 – Senarai Perundangan dan Peraturan

1. Arahan Keselamatan (Semakan dan Pindaan 2017);
2. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi”;
3. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
4. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
5. Pekeliling Am Bilangan 2 Tatacara Pengurusan Aset Alih Kerajaan;
6. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi”;
7. **Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024**
8. **Surat Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022**
9. Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) dalam Perkhidmatan Awam;
10. Surat Pekeliling Perbendaharaan Bil.2 / 1995 (Tambahan Pertama) - “Tatacara Penyediaan, Penilaian dan Penerimaan Tender”;
11. Surat Pekeliling Perbendaharaan Bil. 3 / 1995 - “Peraturan Perolehan Perkhidmatan Perundingan”;
12. Surat Pekeliling Perbendaharaan Bil. 10 / 2010 – “Garis Panduan Pelaksanaan Integrity Pact dalam Perolehan Kerajaan”
13. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA (28 Januari 2019);
14. Akta Tandatangan Digital 1997;
15. Akta Rahsia Rasmi 1972;
16. Akta Jenayah Komputer 1997;
17. Akta Hak Cipta (Pindaan) Tahun 1997;
18. Akta Komunikasi dan Multimedia 1998;

19. Perintah-Perintah Am;
20. Arahan Perbendaharaan;
21. Arahan Teknologi Maklumat 2007;
22. **Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024**
23. Etika Penggunaan E-mel dan Internet Kakitangan Kerajaan; dan
24. Dasar Kriptografi Negara 12 Julai 2013;
25. Peraturan – Peraturan Pegawai Awam (Pelantikan, Kenaikkan Pangkat dan Penamatan Perkhidmatan) 2012;
26. Surat Edaran Ketua Pengarah Keselamatan Kerajaan Bilangan 1 Tahun 2021 : Peringatan Berhubung Kepentingan Melindungi Kerahsiaan Maklumat Kerajaan Dari Ancaman Kebocoran; dan
27. Surat Pekeliling Am Bilangan 1 Tahun 2021 Larangan Penggunaan Telefon Bimbit, Peralatan Komunikasi dan Segala Peralatan Elektronik yang Mampu Merakam Maklumat Dalam Mesyuarat Penting Kerajaan.
28. Pekeliling Am Bilangan 5 Tahun 2021 Tapisan Keselamatan Semula Kepada Pegawai Awam Melalui Sistem e-Vetting;



BANGUNAN IBU PEJABAT KEJORA
Jalan Dato' Haji. Hassan Yunus
81930 Bandar Penawar Johor Darul Ta'zim
Tel: 07-8843000 Faks: 07-8221600
www.kejora.gov.my