POLISI KESELAMATAN SIBER

Kerajaan Negeri Johor

PKS 1.0

POLISI KESELAMATAN SIBER KERAJAAN NEGERI JOHOR

VERSI 1.1

OGOS 2024

ISI KANDUNGAN

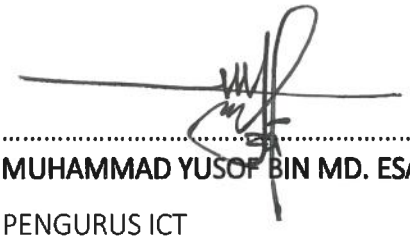
A. SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
SEPTEMBER 2009	1.0	JAWATANKUASA PEMANDU ICT NEGERI JOHOR TAHUN 2009	DISEMBER 2009
SEPTEMBER 2024	1.0	JAWATANKUASA PEMANDU ICT NEGERI JOHOR TAHUN 2024	OGOS 2024

B. REKOD PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
NOVEMBER 2017	2.0	Pindaan keseluruhan bidang keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 Information Security Management System (ISMS)
OGOS 2024	1.0	Pindaan keseluruhan bidang keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2022 Information Security Management System (ISMS)
OGOS 2024	1.0	Pindaan tajuk dokumen dari Dasar Keselamatan ICT Kerajaan Negeri Johor kepada Polisi Keselamatan Siber Kerajaan Negeri Johor
JANUARI 2024	1.1	Pindaan terhadap Senarai Perundangan dan Peraturan-peraturan dengan penambahan Akta Keselamatan Siber 2024

C. KELULUSAN DOKUMEN

BAGI PIHAK SUK KERAJAAN NEGERI JOHOR		
DISEDIAKAN OLEH :		
		
NAMA	:	**MUHAMMAD YUSOF BIN MD. ESA**
JAWATAN	:	PENGURUS ICT
TARIKH	:	01 AUG 2024
DISEMAK OLEH :		
		
NAMA	:	**MOHD FARID BIN HASSAN**
JAWATAN	:	ICTSO NEGERI JOHOR
TARIKH	:	01 AUG 2024
DILULUSKAN OLEH :		
		
NAMA	:	**DATO' HAJI ASHARI BIN HAJI KASNAN**
JAWATAN	:	CDO NEGERI JOHOR
TARIKH	:	01 AUG 2024

D. SINGKATAN

ISTILAH	KETERANGAN / TAKRIFAN
CDO	*Chief Digital Officer* Ketua Pegawai Digital
CSIRT	*Computer Security Incident Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan
ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
ICTSO	*ICT Security Officer* Pegawai Keselamatan Maklumat
IPS	*Intrusion Prevention System* Sistem Pencegah Pencerobohan
ISMS	*Information Security Management System*
JDN	Jabatan Digital Negara
JPICT	Jawatankuasa Pemandu ICT Negeri Johor
LAN	*Local Area Network* Rangkaian Kawasan Setempat
NACSA	National Cyber Security Agency Agensi Keselamatan Siber Negara
PKI	*Public Key Infrastructure* Infrastruktur Kekunci Awam
PKS	Polisi Keselamatan Siber Kerajaan Negeri Johor
PKP	Pelan Kesinambungan Perkhidmatan
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
SLA	*Service Level Agreement* Perjanjian Tahap Perkhidmatan

ISTILAH	KETERANGAN / TAKRIFAN
SLG	*Service Level Guarantee* Jaminan Tahap Perkhidmatan
UPS	*Uninterruptable Power Supply* Bekalan Kuasa Berterusan
CGSO	*Chief Government Security Officer* Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
CSM	*Cybersecurity Malaysia*
JOHOR CSIRT	*Johor Computer Security Incident Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan Johor
AGENSI	Semua Badan Berkanun dan PBT
PBT	Pihak Berkuasa Tempatan
JABATAN	Semua Jabatan Kerajaan Negeri Johor

1.0 PENGENALAN

PKS ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam penggunaan aset ICT. Dokumen ini juga menerangkan kepada semua pengguna dan pembekal di bawah Kerajaan Negeri Johor mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT.

2.0 TUJUAN

Polisi Keselamatan Siber Kerajaan Negeri Johor ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh kakitangan ICT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Johor dalam melindungi maklumat di ruang siber.

3.0 OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

a. Menerangkan kepada semua pengguna merangkumi warga kerja Kerajaan Negeri Johor, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Kerajaan Negeri Johor mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber;

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

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

d. 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

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

4.0 PERNYATAAN

Pengurusan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kerentanan sentiasa berubah.

PKS ini merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah kerahsiaan, integriti dan ketersediaan.

Selain itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada faktor berikut:

a) Penilaian yang bersesuaian dengan perubahan semasa terhadap kerentanan semula jadi aset di bawah Kerajaan Negeri Johor;

b) Ancaman yang wujud akibat daripada kerentanan tersebut; dan

c) Risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

5.0 SKOP

PKS ini merangkumi peraturan-peraturan yang mesti digunakan dalam merancang perlindungan terhadap aset ICT Kerajaan Negeri Johor.

6.0 PRINSIP KESELAMATAN

Prinsip keselamatan hendaklah dipilih berdasarkan penilaian risiko dan kategori data yang dikendalikan oleh sistem seperti yang ditetapkan oleh RAKKSSA. Objektif utama keselamatan maklumat adalah:

a) Kerahsiaan
b) Integriti
c) Ketersediaan
d) Tanpa Sangkalan
e) Pengesahan

Bagi mencapai objektif tersebut prinsip keselamatan berikut hendaklah dipatuhi:

6.1 PRINSIP "PERLU-TAHU"

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

6.2 HAK KEISTIMEWAAN MINIMUM

Pengguna dan pembekal hendaklah diberikan hak keistimewaan minimum untuk menjalankan tugasnya.

6.3 PENGASINGAN TUGAS

Bagi mengekalkan prinsip *checks-and-balances*, Kerajaan Negeri Johor hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

6.4 KAWALAN CAPAIAN BERDASARKAN PERANAN

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

6.5 PEMINIMUMAN DATA

Kerajaan Negeri Johor hendaklah mengamalkan prinsip peminimuman data yang menghadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

7.0 PENILAIAN RISIKO

Kerajaan Negeri Johor hendaklah mengenal pasti risiko terhadap aset ICT. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam aset ICT. Penilaian risiko hendaklah dilaksanakan apabila berlaku sebarang perubahan kepada persekitaran. Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan.

Proses penilaian risiko merangkumi perkara-perkara berikut:

a) **KERENTANAN**

Kerentanan setiap aset ICT hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b) **ANCAMAN**

Kerajaan Negeri Johor hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kerentanan yang telah dikenal pasti.

c) **IMPAK**

Kerajaan Negeri Johor hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi jabatan.

d) **TAHAP RISIKO**

Kerajaan Negeri Johor hendaklah menganggarkan tahap risiko yang ditentukan daripada penemuan ancaman, kebarangkalian dan impak risiko. Kaedah penentuan tahap risiko hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e) **PENGOLAHAN RISIKO**

Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan berdasarkan tiga (3) elemen berikut:

(i) TEKNOLOGI

Teknologi hendaklah dikenal pasti untuk mengelak atau meminimakan risiko.

(ii) PROSES

Kerajaan Negeri Johor hendaklah sekiranya perlu untuk melaksana pengolahan risiko, membangun atau merekayasa bagi:

- Proses
- Manual Prosedur Kerja / *Standard Operating Procedure* (SOP); dan
- Dasar

(iii) MANUSIA

Kerajaan Negeri Johor hendaklah mengenal pasti dan mengurus pengguna dan pembekal yang berkelayakan dan kompeten bagi memastikan pengolahan risiko dilaksanakan secara berkesan.

8.0 PENGURUSAN RISIKO

Kerajaan Negeri Johor hendaklah mengenal pasti struktur tadbir urus pengurusan risiko untuk:

a) Mengenal pasti kerentanan;
b) Mengenal pasti ancaman;
c) Menilai risiko;
d) Menentukan pengolahan risiko;
e) Memantau keberkesanan pengolahan risiko; dan
f) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

Item (e) dan (f) hendaklah dijadikan agenda tetap dan dibincangkan dalam Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Negeri Johor.

BIDANG 1
5.0 KAWALAN ORGANISASI

ORGANIZATIONAL CONTROL

BIDANG 1

5.0 KAWALAN ORGANISASI
ORGANIZATIONAL CONTROL

5.1 POLISI KESELAMATAN MAKLUMAT
Policies for Information Security

OBJEKTIF

Menentukan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Kerajaan Negeri Johor dan perundangan yang berkaitan.

KETERANGAN	TINDAKAN
Pelaksanaan PKS ini akan dijalankan oleh Setiausaha Kerajaan Johor dengan disokong oleh JPICT yang terdiri daripada CDO, ICTSO dan ahli-ahli yang dilantik oleh Setiausaha Kerajaan Johor. PKS hendaklah dipatuhi oleh semua pengguna dan pembekal.	Setiausaha Kerajaan Johor Pengguna Pembekal
Dasar-dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan Kerajaan Negeri Johor kepada pengguna dan pembekal.	ICTSO Negeri
PKS ini perlu dikaji semula secara berkala atau apabila berlaku perubahan kepada aplikasi, prosedur, perundangan dan dasar Kerajaan. Berikut adalah prosedur yang berhubung dengan kajian semula PKS:	ICTSO Negeri JPICT

KETERANGAN	TINDAKAN
a) Mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan JPICT; c) JPICT akan mempertimbangkan dan seterusnya mengesahkan sebarang pindaan yang telah dicadangkan; d) Memaklumkan pindaan yang telah disahkan oleh JPICT kepada semua pengguna dan pembekal; dan e) PKS ini hendaklah dikaji semula mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

Information Security Roles And Responsibities

OBJEKTIF

Menerangkan peranan dan tanggungjawab pengguna yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS ini.

KETERANGAN	TINDAKAN
CHIEF DIGITAL OFFICER NEGERI JOHOR Peranan dan tanggungjawab *Chief Digital Officer* adalah seperti berikut: a) Menguatkuasakan pelaksanaan PKS; b) Memastikan pengguna dan pembekal memahami dan mematuhi peruntukan-peruntukan di bawah PKS;	CDO Negeri

KETERANGAN	TINDAKAN
c) Memastikan semua keperluan organisasi seperti sumber kewangan, personel dan perlindungan keselamatan maklumat adalah mencukupi; d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS; e) Melantik ICTSO Negeri Johor serta memaklumkan pelantikan kepada Ketua Pengarah JDN; f) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; g) Memastikan Pelan Strategik ICT Kerajaan Negeri Johor mengandungi aspek keselamatan ICT; dan h) Menyelaras pelan latihan dan program kesedaran keselamatan ICT.	
ICTSO NEGERI JOHOR Peranan dan tanggungjawab ICTSO Negeri Johor yang dilantik adalah seperti berikut: a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS; b) Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan peraturan dan garis panduan yang berkuat kuasa; c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT	ICTSO Negeri

KETERANGAN	TINDAKAN
dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan ICT kepada NACSA dan seterusnya membantu dalam penyiasatan atau pemulihan; e) Melaporkan insiden keselamatan ICT kepada CDO Negeri Johor bagi insiden yang memerlukan pengaktifan Pelan Kesinambungan Perkhidmatan (PKP); f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; g) Melaksanakan pematuhan PKS oleh pengguna dan pembekal; h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; dan i) Menyedia dan melaksanakan latihan dan program kesedaran keselamatan ICT.	
CDO Jabatan/Agensi Peranan dan tanggungjawab CDO Jabatan/Agensi adalah seperti berikut: a) Memastikan pengguna dan pembekal memahami dan mematuhi peruntukan-peruntukan di bawah PKS; b) Memastikan semua keperluan organisasi seperti sumber	CDO Jabatan / Agensi

KETERANGAN	TINDAKAN
kewangan, personel dan perlindungan keselamatan maklumat adalah mencukupi; c) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; d) Memastikan Pelan Strategik ICT Jabatan/Agensi mengandungi aspek keselamatan ICT; dan e) Menyelaras pelan latihan dan program kesedaran keselamatan ICT; f) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam PKS; dan g) Melantik ICTSO Jabatan/Agensi dan Pengurus ICT serta memaklumkan pelantikan kepada ICTSO Negeri Johor.	
ICTSO Jabatan/Agensi Peranan dan tanggungjawab ICTSO Jabatan/Agensi yang dilantik adalah seperti berikut: a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS; b) Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan peraturan dan garis panduan yang berkuat kuasa; c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta	ICTSO Jabatan / Agensi

KETERANGAN	TINDAKAN
menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan ICT kepada Johor CSIRT dan seterusnya membantu dalam penyiasatan atau pemulihan; e) Melaporkan insiden keselamatan ICT kepada CDO Jabatan / agensi bagi insiden yang memerlukan pengaktifan PKP; f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; g) Melaksanakan pematuhan PKS oleh pengguna dan pembekal; h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT; dan i) Menyedia dan melaksanakan latihan dan program kesedaran keselamatan ICT.	
PENGURUS ICT Peranan dan tanggungjawab Pengurus ICT adalah melaksanakan keperluan PKS dalam operasi semasa seperti berikut: a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan	Pengurus ICT

KETERANGAN	TINDAKAN
teknologi baharu; b) Pembelian atau peningkatan perisian dan sistem komputer; c) Perolehan teknologi dan perkhidmatan komunikasi baharu; dan d) Memastikan pembekal dan rakan usahasama menjalani tapisan keselamatan. **PENTADBIR SISTEM ICT** Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam PKS; c) Memantau aktiviti capaian harian sistem ICT; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menganalisis dan menyimpan rekod jejak audit;	Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
f) Menyediakan laporan mengenai aktiviti capaian secara berkala; g) Memastikan ketersediaan capaian sistem ICT; h) Menjalankan aktiviti *backup* dan *restore* dengan menyediakan SOP; dan i) Memantau setiap perkakasan ICT yang diterima di dalam keadaan yang baik.	
JPICT Peranan dan tanggungjawab JPICT adalah merancang dan menentukan langkah-langkah keselamatan ICT seperti di dalam pekeliling yang berkuat kuasa.	JPICT
JOHOR COMPUTER SECURITY INCIDENT RESPONSE TEAM (Johor CSIRT) Peranan dan tanggungjawab Johor CSIRT adalah seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b) Merekod dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Mengesyorkan Kerajaan Negeri Johor untuk mengambil	ICTSO Johor CSIRT

KETERANGAN	TINDAKAN
tindakan pemulihan dan pengukuhan; e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada jabatan / agensi di bawah Kerajaan Negeri Johor. PENGGUNA Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan menandatangani Surat Akuan Pematuhan PKS; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan Maklumat Rahsia Rasmi; d) Mematuhi prinsip-prinsip PKS dan menjaga kerahsiaan maklumat Kerajaan Negeri Johor; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan;	Pengguna

KETERANGAN	TINDAKAN
iv. Menjaga kerahsiaan maklumat; v. Mematuhi dasar, piawaian dan garis panduan keselamatan ICT yang ditetapkan; vi. Melaksanakan peraturan berkaitan Maklumat Rahsia Rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan kawalan keselamatan ICT dari diketahui umum; viii. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengurus ICT dengan segera; ix. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan x. Bersetuju dengan terma dan syarat yang terkandung di dalam PKS.	

5.3 PENGASINGAN TUGAS

Segregation of Duties

OBJEKTIF

Bagi mengekalkan prinsip *checks-and-balances*, Kerajaan Negeri Johor hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

KETERANGAN	TINDAKAN
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: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang	Ketua Jabatan / Agensi

KETERANGAN	TINDAKAN
digunakan sebagai persekitaran *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan d. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	

5.4 TANGGUNGJAWAB PENGURUSAN

Management Responsibilities

OBJEKTIF

Pengurusan tertinggi perlu memastikan semua pihak mematuhi keselamatan maklumat seperti yang terkandung di dalam polisi dan prosedur di dalam organisasi.

KETERANGAN	TINDAKAN
a) Memastikan pengguna dan pembekal memahami dan mematuhi perundangan, Arahan Perkhidmatan, peraturan dan PKS; dan b) Memastikan pengguna dan pembekal mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Kerajaan Negeri Johor.	CDO Negeri/ Jabatan ICTSO Negeri/ Jabatan

5.5 HUBUNGAN DENGAN PIHAK BERKUASA

Contact With Authorities

OBJEKTIF

Organisasi perlu untuk mengenalpasti kaedah untuk menghubungi dengan pihak berkuasa.

KETERANGAN	TINDAKAN
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab Jabatan/ Agensi; b. Mewujud dan mengemas kini prosedur / senarai pihak berkuasa perundangan / pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia Malaysia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan c. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden. Senarai hubungan pihak berkuasa: i. Jabatan Digital Negara (JDN) ii. Agensi Keselamatan Siber Negara (NACSA)	Ketua Jabatan/ Agensi

KETERANGAN	TINDAKAN
iii. Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) iv. Cyber Security Malaysia (CSM) v. Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) vi. Badan Pengurusan Bangunan vii. Penyedia Perkhidmatan Internet (ISP) viii. Penyedia Perkhidmatan Perkomputeran Awan (CSP) ix. Balai Polis berhampiran x. Balai Bomba berhampiran xi. Hospital berhampiran	

5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

Contact With Special Interest Groups

OBJEKTIF

Organisasi perlu mengenalpasti kaedah perhubungan dengan kumpulan berkepentingan khusus.

KETERANGAN	TINDAKAN
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum bagi: a. meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;	ICTSO

KETERANGAN	TINDAKAN
b. menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c. berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d. berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

5.7 PERISIKAN ANCAMAN

Threat Intelligence

OBJEKTIF

Maklumat yang berkaitan dengan ancaman keselamatan maklumat hendaklah diperolehi dan dianalisa untuk tujuan perisikan.

KETERANGAN	TINDAKAN
Perisikan Ancaman (*Threat Intelligence)* adalah langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman perisikan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Sistem pemantauan (*Security Monitoring*) bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan yang mungkin terjadi di dalam rangkaian atau sistem;	ICTSO

KETERANGAN	TINDAKAN
b) Memasang pendinding api *(Firewall)* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan; c) Setiap data yang disimpan hendaklah di enkripsi (*Encryption*) bagi melindungi data daripada di capai oleh orang tidak sah; d) Memastikan setiap perisian yang digunakan adalah yang terkini dan sentiasa dikemaskini; e) Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh Jabatan / Agensi. f) Membahagikan rangkaian di dalam sesebuah organisasi kepada beberapa bahagian mengikut tingkat atau sebagainya; dan g) Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut keadaan semasa.	

5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

Information Security In Project Management

OBJEKTIF

Keselamatan maklumat perlu diintegrasi dalam pengurusan projek.

KETERANGAN	TINDAKAN
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek; b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenalpasti kawalan-kawalan yang diperlukan; dan d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam PKS.	ICTSO

5.9 MAKLUMAT INVENTORI ASET DAN YANG BERKAITAN

Inventory Of Information And Other Associated Assets

OBJEKTIF

Setiap aset ICT perlu dikenal pasti, diklasifikasi, direkodkan, diselenggara dan dilupuskan apabila tiba masanya berdasarkan kepada tatacara / arahan / peraturan pengurusan aset yang berkuatkuasa dari semasa ke semasa.

KETERANGAN	TINDAKAN
Tanggungjawab yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikenal pasti, diklasifikasi, direkodkan, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh personel yang dibenarkan sahaja; dan c) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	Pegawai Aset Pengguna

5.10 MAKLUMAT PENGGUNAAN ASET YANG BOLEH DITERIMA DAN YANG BERKAITAN

Acceptable Use Of Information And Other Associated Assets

OBJEKTIF

Garis panduan untuk penerimaan aset dan prosedur untuk pengendalian maklumat perlulah dikenalpasti, didokumentasi dan dipatuhi.

KETERANGAN	TINDAKAN
Memastikan semua peraturan pengendalian aset ICT dikenal pasti, didokumenkan dan dilaksanakan.	Pegawai Aset Pengguna

5.11 PEMULANGAN ASET

Return of Assets

OBJEKTIF

Semua pihak perlu memulangkan aset ICT jika berlaku pertukaran ataupun ditamatkan perkhidmatan mengikut kepada peraturan dan terma perkhidmatan organisasi.

KETERANGAN	TINDAKAN
Memastikan semua aset ICT dikembalikan kepada jabatan / agensi mengikut peraturan dan terma perkhidmatan yang ditetapkan sebelum pegawai bertukar, bersara atau penamatan perkhidmatan atau kontrak.	Pegawai Aset Pengguna

5.12 PENGELASAN MAKLUMAT

Classification of Information

OBJEKTIF

Maklumat perlu dikenalpasti mengikut kepada keperluan organisasi berdasarkan kepada kerahsiaan, integriti, ketersediaan dan keperluan pihak yang berkepentingan.

KETERANGAN	TINDAKAN
Maklumat hendaklah dikelaskan sewajarnya oleh Pegawai Pengelas mengikut dokumen Arahan Keselamatan.	Pegawai Pengelas

KETERANGAN	TINDAKAN
Klasifikasi maklumat adalah mengikut kepada Akta 88 - Akta Rahsia Rasmi 1972.	

5.13 PELABELAN MAKLUMAT

Labelling Of Information

OBJEKTIF

Prosedur untuk pelabelan maklumat perlulah dibangunkan dan dilaksanakan mengikut kepada klasifikasi maklumat yang ditetapkan oleh organisasi.

KETERANGAN	TINDAKAN
Prosedur pelabelan maklumat hendaklah dipatuhi mengikut Arahan Keselamatan.	Pengguna

5.14 PENGENDALIAN MAKLUMAT

Handling of Information

OBJEKTIF

Memastikan pergerakan maklumat di antara jabatan / agensi dengan pembekal dilaksanakan mengikut arahan yang sedang berkuatkuasa dari semasa ke semasa.

KETERANGAN	TINDAKAN
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut:	ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
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-langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan merujuk kepada Pekeliling dan Peraturan-peraturan semasa yang berkuat kuasa; dan g) Menjaga kerahsiaan keselamatan maklumat ICT dari didedahkan dan diketahui umum. h) Dasar, prosedur dan kawalan pemindahan maklumat hendaklah diwujudkan.	

5.15 KAWALAN AKSES

Access Control

OBJEKTIF

Menghadkan capaian kepada maklumat dan kemudahan pemprosesan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

KETERANGAN	TINDAKAN
Prosedur kawalan capaian hendaklah diwujudkan, didokumenkan dan dikemaskini berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Perkara berikut perlu dipertimbangkan: a) Keperluan keselamatan sistem jabatan / agensi; b) Kebenaran untuk menyebarkan maklumat; c) Hak capaian dan dasar klasifikasi maklumat sistem dan rangkaian; d) Undang-undang dan peraturan yang berkaitan; e) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; f) Pengasingan peranan kawalan capaian; g) Permohonan rasmi kebenaran capaian; h) Keperluan semakan hak capaian berkala; i) Pembatalan hak capaian; dan j) Arkib semua aktiviti yang berkaitan dengan penggunaan dan pengurusan maklumat pengguna.	ICTSO Pengurus ICT Pentadbir Sistem ICT

5.16 PENGURUSAN IDENTITI

Identity Management

OBJEKTIF

Memastikan pengurusan identiti pengguna, pembekal dan pihak luar yang berurusan dengan organisasi adalah terurus.

KETERANGAN	TINDAKAN
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi : a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi capaian minimum yang akan ditetapkan oleh pemilik sistem; d. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik perkhidmatan digital atau aplikasi terlebih dahulu; e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Penggunaan akaun yang disalahguna dan melanggar peraturan boleh ditarik balik; f. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan	Pengurusan ICT

KETERANGAN	TINDAKAN
g. Pentadbir Sistem Aplikasi / Perkhidmatan Digital boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	

5.17 MAKLUMAT PENGESAHAN DAN PENGURUSAN KATA LALUAN

Authentication Information and Password Management

OBJEKTIF

Pengesahan maklumat perlulah diuruskan dan dikawal termasuk kepada amalan keselamatan terbaik dalam pengendalian maklumat. Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan pemprosesan maklumat.

KETERANGAN	TINDAKAN
Pengguna hendaklah mematuhi garis panduan pengurusan kata laluan yang telah dikuatkuasakan atau mengikut garis panduan jabatan / agensi masing-masing dalam pemilihan, penggunaan dan pengurusan kata laluan untuk melindungi maklumat yang digunakan sebagai pengesahan diri.	Pengguna Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
Pengurusan Kata Laluan Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan berdasarkan garis panduan yang telah ditetapkan: a) Kata laluan hendaklah diingat dan tidak boleh dikongsi, dicatat, disimpan atau didedahkan; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan; c) Kata laluan hendaklah berlainan dengan pengenalan identiti pengguna dan tidak mudah diteka; d) Kombinasi sekurang-kurangnya dua belas (12) aksara dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) kecuali bagi sistem, perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; e) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; f) Sistem hendaklah mempunyai tempoh masa aktif yang akan tamat selepas melebihi tempoh melahu (*idle*) yang ditetapkan seperti tidak melebihi 10 minit atau tertakluk pada penetapan / kekangan sistem / aplikasi masing-masing; g) Sistem yang dibangunkan hendaklah mempunyai kemudahan menukar kata laluan oleh pengguna;	ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
h) Penukaran kata laluan selepas log masuk (login) kali pertama atau selepas reset kata laluan hendaklah dikuat kuasakan; dan i) Kemasukan atau cubaan (*attempt*) kata laluan bagi capaian sistem hendaklah mempunyai had maksimum. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula.	

5.18 HAK AKSES
Access Right

OBJEKTIF

Hak akses perlulah dikawal, disemak, diubahsuai dan dikeluarkan mengikut kepada polisi dan garis panduan yang ditetapkan.

KETERANGAN	TINDAKAN
Prosedur bagi mengurus hak capaian pengguna ke atas sistem dan perkhidmatan hendaklah diwujudkan dan dilaksanakan.	ICTSO Pengurus ICT Pentadbir Sistem ICT

5.19 HUBUNGAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL
Information Security In Supplier Relationship

OBJEKTIF

Proses dan prosedur perlu dikenalpasti dan dilaksana bagi mengurus keselamatan maklumat dan risiko berkaitan dengan pembekal.

KETERANGAN	TINDAKAN
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Kerajaan Negeri Johor. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori; b) Proses kitaran hayat *(lifecycle)* yang seragam untuk menguruskan pembekal; c) Mengawal dan memantau akses pembekal; d) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e) Jenis-jenis obligasi kepada pembekal; f) Pelan kontigensi bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g) Pemakluman Keperluan Keselamatan oleh jabatan/agensi kepada pembekal seterusnya menandatangani Surat Akuan Pematuhan PKS; dan h) Memastikan pembekal melepasi tapisan keselamatan yang ditentukan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).	ICTSO Pengurus ICT Pembekal

5.20 PERJANJIAN KESELAMATAN MAKLUMAT DENGAN PEMBEKAL

Addressing Information Security WithinSupplier Agreements

OBJEKTIF

Keperluan keselamatan maklumat yang berkaitan perlulah dikenalpasti dan dipersetujui dengan semua pembekal berdasarkan kepada kategori pembekal.

KETERANGAN	TINDAKAN
Memastikan pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan jabatan/agensi.	Pengurus ICT Pembekal

5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN KOMUNIKASI MAKLUMAT ICT

Managing Information Security In The Information And Communication Technology (ICT) Supply Chain

OBJEKTIF

Proses dan prosedur perlulah dikenalpasti dan dilaksana untuk menguruskan keselamatan maklumat yang berkaitan produk ICT dan juga rantaian bekalan.

KETERANGAN	TINDAKAN
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat rantaian pembekal bagi menangani risiko berkaitan produk ICT. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut:	ICTSO Pengurus ICT Pembekal

KETERANGAN	TINDAKAN
a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk; dan Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

5.22 PEMANTAUAN, SEMAKAN DAN PERUBAHAN PENGURUSAN PERKHIDMATAN PEMBEKAL

Monitoring, Review And Change Management Of Supplier Services

OBJEKTIF

Organisasi perlu memantau, menyemak, membuat penilaian dan menguruskan perubahan didalam amalan keselamatan maklumat berkaitan pembekal dan servis pembekalan.

KETERANGAN	TINDAKAN
Jabatan / agensi hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;	ICTSO Pengurus ICT Pembekal

KETERANGAN	TINDAKAN
b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan c) Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	
Perkara yang perlu diambil kira adalah seperti berikut: a) Sebarang perubahan hendaklah disemak dan diluluskan oleh Jawatankuasa Pemandu Projek sebelum diterima dan dipinda dalam perjanjian; b) Perubahan yang dilakukan oleh jabatan / agensi bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baharu, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor; dan d) Perubahan hendaklah mempunyai nilai tambah daripada perkhidmatan dan pembekalan sedia ada demi kelangsungan projek.	ICTSO Pengurus ICT Pembekal

5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PERKOMPUTERAN AWAN

Information Security For Use Of Cloud Computing Services

OBJEKTIF

Proses perolehan, penggunaan dan perubahan perkhidmatan awan perlulah dikenalpasti mengikut kepada keperluan keselamatan organisasi.

KETERANGAN	TINDAKAN
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awan yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. a) Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki; b) Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut; c) Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data;	ICTSO Pengurus ICT Pentadbir Sistem ICT Pembekal

KETERANGAN	TINDAKAN
d) Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakupi butiran keselamatan maklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan peraturan pematuhan; e) Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat; f) Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan; g) Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian; h) Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi; dan i) Mematuhi Garis Panduan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam oleh CGSO dan Program Pengkomputeran Awan JDN.	

5.24 PERANCANGAN, PENYEDIAAN DAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Information SecurityIncident Management Planning And Preparation

OBJEKTIF

Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kerentanan apabila berlaku insiden.

KETERANGAN	TINDAKAN
a) Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. b) Pengurusan insiden adalah berdasarkan kepada Pekeliling AM Bilangan 4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam yang sedang berkuat kuasa.	ICTSO Pengurus ICT Johor CSIRT CSIRT Jabatan / Agensi

5.25 PENILAIAN DAN KEPUTUSAN PERISTIWA KESELAMATAN MAKLUMAT

Assessment And Decision On Information Security Events

OBJEKTIF

Organisasi perlu untuk menilai peristiwa keselamatan maklumat dan mengambil keputusan jika peristiwa tersebut adalah insiden keselamatan maklumat.

KETERANGAN	TINDAKAN
Kejadian keselamatan maklumat hendaklah dinilai dan diputuskan untuk diklasifikasikan sebagai insiden keselamatan maklumat.	ICTSO

5.26 MAKLUMBALAS INSIDEN KESELAMATAN MAKLUMAT

Response To Information Security Incident

OBJEKTIF

Insiden keselamatan maklumat perlu diambil tindakan mengikut kepada prosedur yang telah ditetapkan.

KETERANGAN	TINDAKAN
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah berkuat kuasa.	ICTSO Johor CSIRT CSIRT Jabatan / Agensi

5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

Learning From information Security Incidents

OBJEKTIF

Pengetahuan yag diperolehi daripada insiden keselamatan maklumat perlulah digunakan untuk menambahbaik dan juga mempertingkatkan kawalan keselamatan maklumat.

KETERANGAN	TINDAKAN
Iktibar yang diperolehi daripada proses analisis dan penyelesaian kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa hadapan.	ICTSO Pengurus ICT Johor CSIRT CSIRT Jabatan / Agensi

5.28 PENGUMPULAN BUKTI

Collection of Evidence

OBJEKTIF

Organisasi perlu untuk mengenalpasti dan melaksana prosedur untuk kenalpasti pengumpulan perolehan dan penyimpanan semua bukti yang berkaitan dengan insiden keselamatan maklumat.

KETERANGAN	TINDAKAN
Jabatan / agensi hendaklah menentukan prosedur untuk mengenal pasti koleksi, perolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti. Makmal Digital Forensik JDN boleh dirujuk bagi tujuan ini.	ICTSO Pengurus ICT Johor CSIRT CSIRT Jabatan / Agensi

5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN

Information Security During Disruption

OBJEKTIF

Organisasi perlulah merancang bagaimana memastikan keselamatan maklumat sewaktu bencana ataupun gangguan berlaku.

KETERANGAN	TINDAKAN
1. Jabatan / agensi hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, jabatan / agensi perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke	CDO ICTSO Pengurus ICT Pasukan PKP

KETERANGAN	TINDAKAN
atas sistem penyampaian perkhidmatan dan fungsi jabatan / agensi. Jabatan / agensi 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: a. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) jabatan / agensi; b. Menetapkan polisi PKP; c. Mengenal pasti perkhidmatan kritikal; d. Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis — BIA*) dan Penilaian Risiko terhadap perkhidmatan kritikal; e. Membangunkan Pelan PKP; f. Melaksanakan program kesedaran dan latihan pasukan PKP; g. Melaksanakan simulasi ke atas dokumen di para (c); dan h. Melaksanakan penyelenggaraan ke atas pelan di para (c). 2. Jabatan / Agensi hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti berikut:	

KETERANGAN	TINDAKAN
a. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal yang telah dikenal pastiberdasarkan kepada Pelan PKP; b. Melaksanakan *post-mortem* dan mengemaskini pelan-pelan PKP; c. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal; d. Mengemaskini struktur tadbir urus PKP jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP. 3. Jabatan / agensi hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan. 4. Rujuk Pelan Kesinambungan Perkhidmatan (PKP).	

5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN

ICT Readiness For Business Continuity

OBJEKTIF

Memastikan keselamatan maklumat dalam pengurusan kesinambungan perkhidmatan.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan: a) Merancang dan mengenal pasti keperluan keselamatan maklumat; b) Membangun, melaksana, menguji dan menyelenggara pelan kesinambungan perkhidmatan dan pemulihan sistem selepas bencana; dan c) Mematuhi dasar, arahan dan prosedur yang berkuat kuasa.	CDO ICTSO Pengurus ICT Koordinator PKP Pasukan PKP

5.31 UNDANG-UNDANG, BERKANUN, PERATURAN DAN KEPERLUAN KONTRAK

Legal, Statutory, Regulatory And Contractual Requirements

OBJEKTIF

Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

KETERANGAN	TINDAKAN
Keperluan perundangan, peraturan dan perjanjian kontrak yang berkuat kuasa hendaklah dikenal pasti dan dipatuhi oleh pengguna dan pembekal. Senarai Perundangan dan Peraturan-Peraturan yang perlu dipatuhi adalah seperti di lampiran Senarai Perundangan dan Peraturan-Peraturan;	CDO ICTSO Pegawai Undang-undang Pengurus ICT Pentadbir Sistem ICT Pengguna

5.32 HAK HARTA INTELEK

Intellectual Property Rights

OBJEKTIF

Organisasi perlu melaksana prosedur yang sepatutnya untuk melindungi hak harta intelek.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan harta intelek; dan b) Melaksanakan kawalan terhadap keperluan perlesenan di mana mematuhi had pengguna yang telah ditetapkan atau dibenarkan dan hanya menggunakan perisian yang mempunyai lesen yang sah.	CDO ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

5.33 PERLINDUNGAN REKOD

Protection of Records

OBJEKTIF

Rekod perlulah dilindungi daripada hilang, dimusnakan, dipalsukan, diakses oleh pihak yang tidak sepatutnya dan disebarkan tanpa kebenaran.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Keperluan perundangan, peraturan dan perjanjian kontrak; dan	CDO ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
b) Melindungi rekod daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan dengan merujuk Dasar Pengurusan Rekod Kerajaan dan Panduan Pengurusan Rekod Sektor Awam oleh Arkib Negara.	

5.34 PRIVASI DAN PERLINDUNGAN MAKLUMAT PENGENALAN PERIBADI

Privacy And Protection Of Personal Identifiable Information (PII)

OBJEKTIF

Organisasi perlu mengenalpasti dan memenuhi keperluan perlindungan data peribadi mengikut kepada keperluan perundangan dan kontrak.

KETERANGAN	TINDAKAN
Jabatan / agensi hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	CDO ICTSO Pengurus ICT Pengguna

5.35 PENILAIAN BEBAS KESELAMATAN MAKLUMAT

Independent Review of Information Security

OBJEKTIF

Untuk memastikan keselamatan maklumat dilaksanakan mengikut dasar dan prosedur yang ditetapkan.

KETERANGAN	TINDAKAN
Penilaian keselamatan maklumat oleh badan bebas hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	CDO ICTSO Pengurus ICT Pentadbir Sistem ICT

5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

Compliance With Policies,Rules And Standard For Information Security

OBJEKTIF

Pematuhan terhadap polisi, garis panduan berkaitan keselamatan maklumat perlulah sentiasa disemak dan dikemaskini.

KETERANGAN	TINDAKAN
Jabatan / agensi hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan dasar, standard dan keperluan teknikal yang bersesuaian.	CDO ICTSO

5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN

Documented Operating Procedure

OBJEKTIF

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.

KETERANGAN	TINDAKAN
Pengurusan operasi perlu mengambilkira perkara-perkara seperti berikut: a) Semua prosedur keselamatan ICT hendaklah didokumenkan, disimpan, dikawal selia dan boleh dicapai oleh pengguna; b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	ICTSO Pengurus ICT

BIDANG 2
6.0 KAWALAN MANUSIA

PEOPLE CONTROL

BIDANG 2

6.0 KAWALAN MANUSIA
PEOPLE CONTROL

6.1 TAPISAN KESELAMATAN
Screening

OBJEKTIF

Tapisan keselamatan terhadap calon perlulah dilakukan sebelum diterima masuk kedalam organisasi berdasarkan kepada keperluan perundangan dan organisasi, spesifikasi maklumat dan risiko keselamatan.

KETERANGAN	TINDAKAN
Menjalankan tapisan keselamatan terhadap pengguna dan pembekal yang terlibat selaras dengan keperluan perkhidmatan.	Jabatan / Agensi

6.2 TERMA DAN SYARAT PERKHIDMATAN
Terms and Conditions of Employment

OBJEKTIF

Kontrak perkhidmatan perlulah menyatakan tanggungjawab berkaitan keselamatan di dalam organisasi.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna Pembekal

KETERANGAN	TINDAKAN
a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna dan pembekal terlibat dalam menjamin keselamatan aset ICT; dan b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	

6.3 LATIHAN, PENDIDIKAN DAN KESEDARAN KESELAMATAN MAKLUMAT

Information Security Awareness, Education and Training

OBJEKTIF

Semua warga kerja dan pihak berkepentingan di dalam organisasi perlulah menerima program kesedaran, pendidikan dan latihan berkaitan polisi dan prosedur keselamatan maklumat terutama yang berkaitan dengan skop tugas.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber Kerajaan Negeri Johor, Sistem Pengurusan Keselamatan (ISMS) dan latihan teknikal yang berkaitan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;	Pengguna Pembekal Pengurus ICT

KETERANGAN	TINDAKAN
b) Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber Kerajaan Negeri Johor perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	

6.4 PROSES TATATERTIB

Disciplinary Process

OBJEKTIF

Proses tindakan tatatertib perlulah diseragamkan dan dikomunikasikan kepada kakitangan dan pihak berkepentingan yang melanggar polisi keselamatan maklumat.

KETERANGAN	TINDAKAN
Sebarang pelanggaran terhadap perundangan, Arahan Perkhidmatan, peraturan dan PKS yang ditetapkan oleh Kerajaan Negeri Johor boleh dikenakan tindakan tatatertib.	Pengguna Pembekal

6.5 TANGGUNGJAWAB APABILA PENAMATAN ATAU PERTUKARAN PERKHIDMATAN

Termination or Change of Employment Responsibilities

OBJEKTIF

Memelihara kepentingan Kerajaan Negeri Johor apabila berlaku pertukaran, penamatan perkhidmatan dan perubahan bidang tugas pengguna dan pembekal.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pekeliling-pekeliling berkaitan penamatan atau pertukaran perkhidmatan; b) Memastikan semua aset ICT dikembalikan kepada jabatan / agensi mengikut peraturan dan terma perkhidmatan yang ditetapkan; dan c) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat.	ICTSO Pentadbir Sistem ICT Pegawai Aset Pengguna

6.6 KERAHSIAAN ATAU DOKUMEN PERJANJIAN KERAHSIAAN

Confidentiality or Non-Disclosure Agreements

OBJEKTIF

Kerahsian atau perjanjian bukan pendedahan yang berkaitan dengan organisasi perlulah dikenalpasti, didokumenkan, disemak dan ditandatangan oleh warga kerja dan semua pihak yang berkepentingan.

KETERANGAN	TINDAKAN
Syarat-syarat perjanjian kerahsiaan atau maklumat terperingkat perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO Pengurus ICT Pembekal

6.7 KERJA JARAK JAUH
Remote Working

OBJEKTIF

Langkah keselamatan perlulah dilaksanakan apabila warga kerja bekerja dari luar premis dalam mengakses, memproses dan menyimpan maklumat organisasi.

KETERANGAN	TINDAKAN
a) Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian daripada sistem rangkaian dalaman; dan ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *teleworking*. b) Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*); c) Lokasi bagi akses ke rangkaian dalaman hendaklah dipastikan selamat; d) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Ketua Jabatan/ Agensi. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan	ICTSO Pentadbir Sistem ICT Ketua Jabatan/ Agensi Pengguna

KETERANGAN	TINDAKAN
e) Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan/ agensi.	

6.8 PELAPORAN KESELAMATAN MAKLUMAT

Information Security Event Reporting

OBJEKTIF

Organisasi perlulah menyediakan kaedah kepada pengguna untuk melaporkan peristiwa yang mencurigakan berkaitan keselamatan maklumat melalui platfom rasmi mengikut tempoh masa yang sesuai.

KETERANGAN	TINDAKAN
Insiden keselamatan maklumat atau ancaman yang berlaku hendaklah dilaporkan sebagaimana prosedur pelaporan insiden keselamatan maklumat yang berkuat kuasa.	ICTSO Pengurus ICT Johor CSIRT CSIRT Jabatan / Agensi
Pengguna dan pembekal sistem jabatan / agensi dikehendaki mengambil maklum dan melaporkan kerentanan keselamatan maklumat kepada Pentadbir Sistem ICT.	Pentadbir Sistem ICT Pengguna Pembekal

BIDANG 3
7.0 KAWALAN FIZIKAL

PHYSICAL CONTROL

BIDANG 3

7.0 KAWALAN FIZIKAL
PHYSICAL CONTROL

7.1 LINGKUNGAN KESELAMATAN FIZIKAL

Physical Security Parameter

OBJEKTIF

Lingkungan keselamatan fizikal perlulah dikenalpasti untuk melindungi kawasan yang mengandungi maklumat dan juga aset yang berkaitan.

KETERANGAN	TINDAKAN
Mengenal pasti lingkungan keselamatan dan menentukan tahap perlindungan keselamatan yang diperlukan untuk melindungi Maklumat Rahsia Rasmi dan kemudahan pemprosesan maklumat berdasarkan kepada Arahan Keselamatan. Kawalan kawasan terperingkat adalah bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat. Perkara yang perlu dipatuhi termasuk yang berikut: a) Ketua Jabatan hendaklah melantik Pegawai Keselamatan Jabatan (PKJ) yang bertanggungjawab mengenai pentadbiran Jabatan bagi melaksanakan arahan-arahan keselamatan dengan mendapat nasihat Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO);	ICTSO Pegawai Keselamatan Jabatan / Agensi

KETERANGAN	TINDAKAN
b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, jeriji besi, sistem kawalan pintu, kamera litar tertutup dan pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Garis Panduan Kawalan Keselamatan Fizikal Premis hendaklah diwujud, dikemaskini dan dilaksanakan mengikut Arahan Keselamatan serta merujuk khidmat nasihat Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); d) Melindungi tempat terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini dengan merekodkan akses untuk tujuan keselamatan dan pengauditan; e) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; f) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan dan ancaman manusia; g) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam tempat terperingkat; h) Sebarang pemasangan peralatan kawalan capaian pintu dan kamera litar tertutup perlulah mengikut	

KETERANGAN	TINDAKAN
standard serta piawaian Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) dan mendapat pengesahan Pegawai Keselamatan Jabatan; dan i) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada mana-mana pihak yang tidak diberi kebenaran memasukinya.	

7.2 KAWALAN KEMASUKAN FIZIKAL

Physical Entry Control

OBJEKTIF

Kawasan larangan perlulah dilindungi dari akses keluar dan masuk fizikal.

KETERANGAN	TINDAKAN
Kawasan larangan hendaklah dilindungi dengan kawalan kemasukan berdasarkan Arahan Keselamatan dan kawalan keselamatan fizikal bangunan jabatan / agensi.	ICTSO Pegawai Keselamatan Jabatan / Agensi

7.3 KAWALAN PEJABAT, BILIK DAN TEMPAT OPERASI

Securing Offices, Rooms and Facilities

OBJEKTIF

Keselamatan fizikal untuk pejabat, bilik dan kemudahan perlulah direkabentuk dan dilaksanakan.

KETERANGAN	TINDAKAN
Kawalan fizikal bagi ruang pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan berdasarkan Arahan Keselamatan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kawasan tempat berkerja, bilik mesyuarat, bilik krisis, bilik bincang, bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	ICTSO Pengurus ICT Pegawai Keselamatan Jabatan / Agensi

7.4 PEMANTAUAN KESELAMATAN FIZIKAL

Physical Security Monitoring

OBJEKTIF

Premis perlulah sentiasa dipantau dari akses keluar dan masuk oleh pihak yang tidak dibenarkan.

KETERANGAN	TINDAKAN
Akses fizikal ke premis hendaklah dikawal dan dipantau setiap masa daripada pihak yang tidak dikenali atau sebarang aktiviti yang mencurigakan. Langkah-langah berikut boleh dipertimbangkan bagi pemantauan keselamatan fizikal : a) Memastikan premis disediakan dengan sistem pemantauan komprehensif seperti pengawal	ICTSO Pegawai Keselamatan Jabatan / Agensi

KETERANGAN	TINDAKAN
keselamatan, alat penggera pencerobohan, *Closed-Circuit Television (CCTV)* dan Sistem Pengurusan Maklumat Keselamatan Fizikal; b) Sistem pemantauan fizikal hendaklah dilindungi daripada sebarang ancaman yang boleh menjejaskan fungsi atau keselamatan maklumat Kerajaan Negeri Johor; c) Sistem pemantauan fizikal hendaklah diuji secara berkala bagi memastikan ketersediaan fungsinya semasa kecemasan; dan d) Tempoh pengekalan rekod pemantauan fizikal adalah sekurang-kurangnya lima (5) tahun.	

7.5 PERLINDUNGAN TERHADAP ANCAMAN LUARAN DAN PERSEKITARAN

Protecting Against External and Environmental Threat

OBJEKTIF

Perlindungan daripada ancaman luaran dan persekitaran seperti bencana alam atau kemalangan perlulah dikenalpasti dan dilaksanakan.

KETERANGAN	TINDAKAN
Perlindungan fizikal perlu direka bentuk dan dilaksanakan bagi menghadapi bencana alam, ancaman luar dan kemalangan berdasarkan Arahan Keselamatan dan peraturan-peraturan yang berkuat kuasa.	ICTSO Pegawai Keselamatan Jabatan / Agensi Koordinator PKP

7.6 BERTUGAS DALAM KAWASAN LARANGAN

Working in Secured Area

OBJEKTIF

Langkah keselamatan bekerja dikawasan larangan perlulah dikenalpasti dan dilaksanakan.

KETERANGAN	TINDAKAN
Prosedur bertugas di kawasan larangan perlu direka bentuk dan dilaksanakan berdasarkan Arahan Keselamatan dan peraturan-peraturan yang berkuat kuasa.	ICTSO Pegawai Keselamatan Jabatan / Agensi

7.7 DASAR MEJA BERSIH DAN SKRIN BERSIH

Clear Desk and Clear Screen

OBJEKTIF

Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

KETERANGAN	TINDAKAN
Akses fizikal ke premis hendaklah dikawal dan dipantau setiap masa daripada pihak yang tidak dikenali atau sebarang aktiviti yang mencurigakan. Langkah-langah berikut boleh dipertimbangkan bagi pemantauan keselamatan fizikal : a) Memastikan premis disediakan dengan sistem pemantauan komprehensif seperti pengawal keselamatan, alat penggera pencerobohan, *Closed-*	ICTSO Pengurus ICT Pengguna

KETERANGAN	TINDAKAN
Circuit Television (CCTV) dan Sistem Pengurusan Maklumat Keselamatan Fizikal; b) Sistem pemantauan fizikal hendaklah dilindungi daripada sebarang ancaman yang boleh menjejaskan fungsi atau keselamatan maklumat Kerajaan Negeri Johor; c) Sistem pemantauan fizikal hendaklah diuji secara berkala bagi memastikan ketersediaan fungsinya semasa kecemasan; dan d) Tempoh pengekalan rekod pemantauan fizikal adalah sekurang-kurangnya lima (5) tahun.	

7.8 PENEMPATAN DAN PERLINDUNGAN ASET ICT

Equipment Siting and Protection

OBJEKTIF

Aset ICT perlulah ditempatkan dan dilindungi daripada sebarang ancaman.

KETERANGAN	TINDAKAN
Aset ICT hendaklah ditempatkan dan dilindungi untuk meminimumkan risiko ancaman dan pencerobohan. Prosedur penempatan dan perlindungan aset ICT hendaklah diwujudkan serta dilaksanakan.	ICTSO Pegawai Aset Pegawai Keselamatan Jabatan / Agensi

7.9 KESELAMATAN ASET ICT DI LUAR PREMIS

Security of Equipment Off-Premises

OBJEKTIF

Aset ICT yang dibawa keluar dari premis hendaklah sentiasa dilindungi.

KETERANGAN	TINDAKAN
Aset ICT yang dibawa keluar hendaklah mematuhi perkara-perkara berikut: a) Aset ICT hendaklah dilindungi dan dikawal sepanjang masa; dan b) Penyimpanan atau penempatan aset ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pegawai Aset Pengguna Pembekal

7.10 PENGENDALIAN MEDIA

Media handling

OBJEKTIF

Media storan perlulah diuruskan dari segi proses perolehan, penggunaan, pengangkutan dan pelupusan mengikut kepada klasifikasi dan pengendalian pengurusan maklumat.

KETERANGAN	TINDAKAN
PENGURUSAN MEDIA MUDAH ALIH Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh jabatan / agensi. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:	ICTSO Ketua Jabatan / Agensi Pengurus ICT Pegawai Aset Pengguna

KETERANGAN	TINDAKAN
a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepadapengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e) Menyimpan semua jenis media di tempat yang selamat. PELUPUSAN MEDIA Prosedur pelupusan media adalah seperti berikut: a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh jabatan / agensi; dan b) Media yang mengandungi maklumat terperingkat hendaklah disanitasi terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa;	

KETERANGAN	TINDAKAN
PEMINDAHAN MEDIA FIZIKAL Prosedur pemindahan media fizikal adalah sperti berikut: a) Pemindahan media fizikal keluar premis perlu mendapat kelulusan dan mengikut kaedah pemindahan aset ICT yang ditetapkan oleh jabatan / agensi; dan b) Media yang mengandungi maklumat terperingkat hendaklah disanitasi terlebih dahulu sebelum dipindahkan mengikut prosedur yang berkuat kuasa. Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Aset ICT yang dibawa untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan aset ICT : a) Aset ICT yang dibawa keluar dari premis jabatan / agensi mestilah mendapat kelulusan Pegawai Aset atau Ketua Bahagian/Unit atau Pengurus ICT dan tertakluk kepada tujuan yang dibenarkan; b) Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	

7.11 UTILITI SOKONGAN

Supporting Utility

OBJEKTIF

Aset ICT perlulah dilindungi daripada gangguan bekalan kuasa dan gangguan lain yang disebabkan oleh utiliti sokongan.

KETERANGAN	TINDAKAN
Aset ICT perlu dilindungi dari kegagalan bekalan kuasa dengan menggunakan utiliti sokongan. Utiliti sokongan hendaklah diselenggara dan diuji secara berkala.	ICTSO Pegawai Keselamatan Jabatan / Agensi

7.12 KESELAMATAN KABEL

Cabling Security

OBJEKTIF

Kabel bekalan kuasa, data dan kabel sokongan yang lain perlulah dilindungi daripada pintasan, gangguan dan kerosakan.

KETERANGAN	TINDAKAN
Kabel elektrik dan kabel telekomunikasi yang membawa data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah yang perlu diambil adalah seperti yang berikut : a) Menggunakan kabel yang mengikut spesifikasi yang ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan	Pengurus ICT Pentadbir Sistem Operasi Pegawai Keselamatan Jabatan/Agensi

KETERANGAN	TINDAKAN
c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.13 PENYELENGGARAAN ASET ICT

Equipment Maintenance

OBJEKTIF

Peralatan hendaklah diselenggara dengan baik untuk memastikan ketersediaan integriti dan kerahsian maklumat.

KETERANGAN	TINDAKAN
Aset ICT perlu diselenggara dengan baik untuk memelihara ketersediaan dan kebolehgunaan.	Pegawai Aset Pentadbir Sistem ICT

7.14 PELUPUSAN YANG SELAMAT DAN GUNA SEMULA ASET ICT

Secure Disposal or Re-use of Equipment

OBJEKTIF

Peralatan yang mengandungi media storan perlulah disahkan untuk memastikan sebarang data yang sensitif dan perisian yang berlesen dikeluarkan sebelum dilupuskan.

KETERANGAN	TINDAKAN
Aset ICT yang mengandungi media storan hendaklah disahkan untuk memastikan sebarang data yang sensitif dan perisian berlesen telah dihapuskan atau *overwritten* secara selamat mengikut peraturan-peraturan yang berkuat kuasa sebelum dilupuskan atau diguna semula. Aset ICT yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuatkuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan jabatan / agensi. Langkah-langkah seperti berikut hendahlah diambil: a) Peralatan ICT yang akan dilupuskan sebelum dipindah milik perlu dipastikan bahawa data-data dalam storan hendaklah telah dihapuskan dengan cara yang selamat; b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c) Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa; e) Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia didalam komputer disalin	Pengurus ICT Pegawai Aset Pengguna

KETERANGAN	TINDAKAN
pada media storan kedua seperti *disket* atau *thumbdrive* atau apa-apa media storan berkaitan sebelum menghapuskan maklumat daripada peralatan komputer yang hendak dilupuskan; f) Data dan maklumat dalam aset ICT yang dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal; sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; g) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling Tatacara Pengurusan Aset Alih Kerajaan yang berkuatkuasa; h) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan sepertimana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan i) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT.	

BIDANG 4
8.0 KAWALAN TEKNOLOGI

TECHNOLOGY CONTROL

BIDANG 4

8.0 KAWALAN TEKNOLOGI
TECHNOLOGY CONTROL

8.1 PERANTI AKHIR PENGGUNA
User End Point Devices

OBJEKTIF

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.

KETERANGAN	TINDAKAN
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: a) Tamatkan sesi aktif apabila selesai tugas; b) *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Pengguna

8.2 PENGURUSAN HAK CAPAIAN ISTIMEWA

Management of Privileged Access Rights

OBJEKTIF

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan terurus.

KETERANGAN	TINDAKAN
Penetapan dan penggunaan ke atas hak capaian *privilege* hendaklah dikawal selia, dipantau dan dikemaskini berdasarkan keperluan skop tugas.	Pengurus ICT Pentadbir Sistem ICT

8.3 SEKATAN CAPAIAN MAKLUMAT

Information Access Restriction

OBJEKTIF

Akses kepada maklumat dan aset lain yang berkaitan hendaklah dihadkan dan diselaraskan dengan dasar khusus topik mengenai kawalan akses.

KETERANGAN	TINDAKAN
Capaian kepada fungsi maklumat dan sistem hendaklah dihadkan mengikut tetapan capaian sistem dan rangkaian. Capaian maklumat terhad kepada pengguna dan untuk tujuan yang dibenarkan.	Pengurus ICT Pentadbir Sistem ICT

8.4 KAWALAN CAPAIAN KEPADA KOD SUMBER

Access Control to Program Source Code

OBJEKTIF

Akses kepada baca dan tulis kod sumber, alat pembangunan dan perisian perpustakaan (*library*) hendaklah diuruskan dengan sewajarnya.

KETERANGAN	TINDAKAN
Capaian kepada *source code* hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Log audit hendaklah dikekalkan kepada semua capaian *source code*; b) Penyelenggaraan dan penyalinan *source code* hendaklah tertakluk kepada kawalan perubahan; dan c) *Source code* bagi semua sistem dan perisian aplikasi yang yang dibangunkan oleh jabatan / agensi negeri Johor disarankan untuk menjadi hakmilik Kerajaan Negeri Johor.	ICTSO Pengurus ICT Pentadbir Sistem ICT

8.5 PENGESAHAN KESELAMATAN

Secure Authentication

OBJEKTIF

Teknologi dan prosedur pengesahan keselamatan hendaklah dilaksanakan berdasarkan sekatan capaian maklumat dan dasar khusus topik pada kawalan akses.

KETERANGAN	TINDAKAN
Kawalan capaian terhadap sistem aplikasi 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: a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan / agensi; b) Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap sistem aplikasi; c) Mengawal capaian ke atas sistem aplikasi menggunakan prosedur log masuk yang terjamin; d) Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan f) Mewujudkan jejak audit ke atas semua capaian sistem aplikasi.	ICTSO Pengurus ICT Pentadbir Sistem ICT

8.6 PENGURUSAN KAPASITI

Capacity Management

OBJEKTIF

Penggunaan sumber hendaklah dipantau dan diselaraskan mengikut arus dan keperluan kapasiti yang dijangkakan.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kapasiti komponen aset ICT hendaklah dirancang, diurus dan dikawal dengan teliti bagi memastikan keperluannya mencukupi dan bersesuaian untuk pembangunan dan kegunaan pada masa hadapan; dan b) Keperluan kapasiti hendaklah mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko.	ICTSO Pengurus ICT Pentadbir Sistem ICT

8.7 KAWALAN TERHADAP PERISIAN HASAD

Controls Againts Malware

OBJEKTIF

Perlindungan terhadap perisian hasad hendaklah dilaksanakan dan disokong oleh kesedaran pengguna yang bersesuaian.

KETERANGAN	TINDAKAN
Tindakan seperti berikut hendaklah dilaksanakan: a) Memasang perkakasan dan perisian keselamatan untuk mengesan perisian hasad mengikut prosedur penggunaan yang betul dan selamat;	Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

KETERANGAN	TINDAKAN
b) Memasang dan menggunakan hanya perisian aplikasi yang tulen, berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuat kuasa; c) Mengimbas perisian dengan antivirus sebelum menggunakannya; d) Mengemaskini antivirus dengan versi terkini; e) Menyemak kandungan sistem secara berkala bagi mengesan aktiviti yang tidak diingini; f) Memasukkan klausa waranti di dalam kontrak yang telah ditawarkan kepada pembekal; g) Mengadakan program dan prosedur jaminan kualiti perisian dan sistem; dan h) Menghadiri program kesedaran keselamatan ICT.	

8.8 PENGURUSAN KERENTANAN TEKNIKAL

Management of Technical Vulnerability

OBJEKTIF

Maklumat tentang kelemahan teknikal sistem aplikasi dalam penggunaan hendaklah diperolehi, pendedahan organisasi kepada kelemahan tersebut hendaklah dinilai dan langkah-langkah yang sewajarnya hendaklah diambil.

KETERANGAN	TINDAKAN
Perkara-perkara perlu dipatuhi:	Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
a) Melaksanakan ujian penembusan sekurang-kurangnya sekali untuk memperolehi maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; b) Menganalisis tahap risiko kerentanan; dan c) Mengambil tindakan pengolahan dan kawalan risiko.	

8.9 PENGURUSAN KONFIGURASI

Configuration Management

OBJEKTIF

Konfigurasi termasuk konfigurasi keselamatan, perkakasan, perisian, perkhidmatan dan rangkaian hendaklah diwujudkan, didokumenkan, dilaksanakan, dipantau dan disemak.

KETERANGAN	TINDAKAN
Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana sepatutnya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak kakitangan penyelenggaraan dan/atau pembekal: a) Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaikuntuk mengkonfigurasi aset perkakasan dan perisian;	Pentadbir Sistem ICT Pembekal

KETERANGAN	TINDAKAN
b) Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya; c) Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan prosedur yang berkaitan; d) Perlu diingat keperluan utama unik organisasi terutamanya dalam hal konfigurasi keselamatan termasuk kebolehlaksanaan untuk menggunakan atau mengurus templat pada bila-bila masa; dan e) Disemak pada selang masa yang sesuai untuk memenuhi kemas kinisistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku.	

8.10 PEMADAMAN MAKLUMAT

Information Deletion

OBJEKTIF

Maklumat yang disimpan dalam sistem aplikasi, peranti atau dalam mana-mana yang lain media storan hendaklah dipadamkan apabila tidak diperlukan lagi.

KETERANGAN	TINDAKAN
Organisasi harus sedar tentang kewajipan mereka untuk memadamkandata yang disimpan pada media storan apabila ia tidak lagi diperlukan dengan: a) Pilih kaedah pemadaman yang sesuai yang mematuhi mana-manaundang-undang atau peraturan sedia ada.	Pentadbir Sistem ICT Pegawai Aset Pengguna

KETERANGAN	TINDAKAN
Pilihan termasuk pemadaman biasa, tulis ganti atau penghapusan dikodkan. b) Rekodkan hasil penyingkiran untuk rujukan masa hadapan. c) Pastikan bahawa apabila menggunakan pembekal pemadaman khusus, organisasi memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa pemadaman telah dilakukan. Organisasi harus menyatakan dengan tepat keperluan mereka apabila menggunakan pihak ketiga, termasuk kaedah pemadaman dan jangka masa, dan harus menjamin bahawa terma aktiviti pemadaman dimasukkan dalam kontrak perjanjian.	

8.11 *DATA MASKING*

Data Masking

OBJEKTIF

Data Masking hendaklah digunakan oleh organisasi mengikut dasar khusus topik mengenai kawalan akses dan khusus topik lain yang berkaitan dasar, dan keperluan perniagaan, mengambil perundangan yang terpakai ke dalam pertimbangan.

KETERANGAN	TINDAKAN
Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan perkara-perkara seperti berikut:	Pentadbir Sistem Aplikasi

KETERANGAN	TINDAKAN
a) Tahap penyamaran dan/atau penyamaran yang diperlukan berbanding dengan sifat data; b) Cara *Data Masking* sedang diakses; c) Sebarang perjanjian mengikat yang menyekat penggunaan data untuk disembunyikan; d) Mengekalkan penyamaran data berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah; dan e) Meneliti data yang diterima dan bagaimana ia telah diberikankepada mana-mana sumber dalaman atau luaran.	

8.12 PENCEGAHAN KEBOCORAN DATA

Data Leakage Prevention

OBJEKTIF

Langkah pencegahan kebocoran data hendaklah digunakan pada sistem aplikasi, kerja bersih dan mana-mana peranti lain yang memproses, menyimpan atau menghantar yang sensitif.

KETERANGAN	TINDAKAN
Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi mereka, organisasi harus:	Pengurus ICT Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
a) Klasifikasikan data selaras dengan piawaian industri yangdiiktiraf (PII, data komersial, maklumat produk), untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian; b) Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. e-mel,pemindahan fail dalaman dan luaran, peranti USB); c) Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke/dan dari platform dan sistem aplikasi tertentu; d) Kebenaran daripada pemilik data sebelum sebarang pemindahan data dilaksanakan; e) Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar*monitor* yang memaparkan jenis data yang dilindungi; f) Sulitkan sandaran data yang mengandungi maklumat sensitif; g) Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada faktor luaran seperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP; dan	

KETERANGAN	TINDAKAN
h) Memastikan perisian *operating system* dan antivirus sentiasa dikemaskini.	

8.13 SANDARAN MAKLUMAT

Information Backup

OBJEKTIF

Salinan sandaran maklumat, perisian dan sistem aplikasi hendaklah diselenggara dan diuji secara berkala mengikut dasar khusus topik yang dipersetujui pada sandaran.

KETERANGAN	TINDAKAN
Perkara berikut hendaklah dilaksanakan bagi memastikan sistem aplikasi dapat dipulihkan: a) Membuat sandaran penuh ke atas semua sistem aplikasi dan perisian sekurang-kurangnya satu kali atau terdapat perubahan versi terbaharu; b) Membuat sandaran ke atas semua data dan maklumat secara harian, mingguan, bulanan dan tahunan; c) Menguji sistem sandaran sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan; dan d) Salinan sandaran hendaklah disimpan di lokasi berlainan yang selamat.	Pengurus ICT Pentadbir Sistem ICT Pengguna

8.14 REDUNDANSI FASILITI PERKHIDMATAN

Redundancy of Information Processing Facilities

OBJEKTIF

Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan redundansi mencukupi untuk memenuhi keperluan ketersediaan.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan: a) Memastikan fasiliti perkhidmatan mempunyai mekanisma *r*edundansi yang mencukupi; dan b) Memastikan pengujian keberkesanan dilakukan dari semasa ke semasa.	Pengurus ICT Pentadbir Sistem ICT Koordinator PKP

8.15 LOG DAN PEMANTAUAN

Logging and Monitoring

OBJEKTIF

Log yang merekodkan aktiviti, pengecualian, kesalahan dan peristiwa lain yang berkaitan hendaklah dihasilkan, disimpan, dilindungi dan dianalisis. Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Fail log hendaklah diaktifkan dan disimpan untuk tempoh yang dipersetujui;	ICTSO Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem aplikasi dan mengambil tindakan membaik pulih dengan segera; dan d) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, laporan hendaklah dibuat kepada ICTSO untuk tindakan selanjutnya. Fasiliti log dan maklumat log hendaklah dilindungi daripada perkara berikut: a) Kemudahan merekod dan menyimpan maklumat hendaklah dilindungi daripada diubahsuai; b) Melindungi maklumat log daripada capaian yang tidak dibenarkan; dan c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem aplikasi dan mengambil tindakan membaik pulih dengan segera.	

8.16 AKTIVITI PEMANTAUAN
Monitoring Activities

OBJEKTIF

Rangkaian dan sistem aplikasi hendaklah dipantau untuk anomali tingkah laku dan tindakan yang sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat.

KETERANGAN	TINDAKAN
a) Aktiviti aplikasi, sistem, storan, media, rangkaian dan *end-point devices* hendaklah dipantau untuk mengenalpasti tindakan anomali yang berlaku. Ia adalah bagi membolehkan tindakan sewajarnya dapat diambil untuk menilai potensi insiden keselamatan maklumat. b) Skop dan tahap pemantauan ditentukan mengikut keperluan Jabatan / agensi, peraturan dan prosedur yang berkaitan. c) Maklumat pemantauan adalah seperti berikut: i. Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke/ dari aplikasi; ii. Akses kepada platform kritikal organisasi, adalah tidak terhad kepada Sistem, Pelayan, Perkakasan rangkaian iii. Fail konfigurasi sistem dan rangkaian pelbagai peringkat; iv. Log peralatan rangkaian; v. Log kejadian *(events log)* berkaitan aktiviti sistem dan rangkaian; vi. Semakan kod yang sedang digunakan hendaklah kod yang dibenarkan ke atas sistem dan tidak mengganggu operasi sistem; dan vii. Penggunaan sumber dan prestasinya.	CDO ICTSO Pengurus ICT Pentadbir Sistem ICT

8.17 KESERAGAMAN WAKTU

Clock Synchronisation

OBJEKTIF

Jam sistem pemprosesan maklumat yang digunakan oleh organisasi hendaklah disegerakkan kepada sumber masa yang diluluskan.

KETERANGAN	TINDAKAN
Waktu sistem pemprosesan maklumat atau domain keselamatan hendaklah diselaraskan mengikut sumber piawaian waktu negara.	Pentadbir Sistem ICT

8.18 PENGGUNAAN PROGRAM KEISTIMEWAAN UTILITI

Use of Privileged Utility Programs

OBJEKTIF

Penggunaan program keistimewaan utiliti yang boleh mengatasi sistem dan kawalan aplikasi hendaklah dihadkan dan dikawal ketat.

KETERANGAN	TINDAKAN
Penggunaan program keistimewaan utiliti hendaklah dikawal selia dengan baik.	ICTSO Pengurus ICT

8.19 PEMASANGAN PERISIAN PADA SISTEM PENGOPERASIAN

Installation of Software on Operational System

OBJEKTIF

Prosedur dan langkah hendaklah dilaksanakan untuk mengurus dengan selamat pemasangan perisian pada sistem pengoperasian.

KETERANGAN	TINDAKAN
a) Pemasangan dan pengemaskinian perisian hanya boleh dilakukan setelah mendapat kelulusan Pentadbir Sistem Aplikasi dan Pentadbir Sistem Operasi; b) Penggunaan perisian dan sistem pengoperasian hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; c) Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat kelulusan dari Pentadbir Sistem Aplikasi dan Pentadbir Sistem Operasi; d) Memastikan penggunaan perisian mempunyai lesen sah; dan e) Satu strategi *rollback* harus diadakan sebelum perubahan dilaksanakan.	Pengurus ICT Pentadbir Sistem ICT

8.20 KAWALAN RANGKAIAN

Network Control

OBJEKTIF

Rangkaian dan peranti rangkaian hendaklah dilindungi, diurus dan dikawal untuk melindungi maklumat dalam sistem dan aplikasi.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi:	Pengurus ICT Pentadbir Sistem Operasi Pengguna

KETERANGAN	TINDAKAN
a) Memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b) Perkakasan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari sebarang risiko; c) Capaian rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d) Semua perkakasan rangkaian hendaklah mempunyai pengesahan daripada pihak berkuasa sebelum proses pemasangan dan konfigurasi; e) Perkakasan keselamatan rangkaian hendaklah dipasang, dikonfigurasi dan diselia; f) Pemasangan *sniffer* atau *network analyzer* hendaklah mendapat kebenaran daripada Pengurus ICT; g) Sebarang penyambungan rangkaian perlu mendapat kelulusan Pengurus ICT; h) Penggunaan *broadband* persendirian adalah dilarang ke atas aset ICT; i) Kemudahan bagi wireless LAN hendaklah mendapat kelulusan daripada Pengurus ICT; j) Perjanjian perkhidmatan rangkaian hendaklah mempunyai *Services Level Assurance (SLA)*;	

KETERANGAN	TINDAKAN
k) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; l) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; dan m) Mewujud dan melaksana kawalan pengalihan laluan *(routing control)* jika bekeperluan bagi memastikan pematuhan terhadap peraturan Jabatan / Agensi.	

8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN

Security of Network Services

OBJEKTIF

Mekanisme keselamatan, tahap perkhidmatan dan keperluan perkhidmatan rangkaian perkhidmatan hendaklah dikenal pasti, dilaksanakan dan dipantau.

KETERANGAN	TINDAKAN
Semua perkhidmatan rangkaian hendaklah mngikut amalan terbaik keperluan keselamatan rangkaian.	Pentadbir Sistem Operasi

8.22 PENGASINGAN RANGKAIAN

Segregation in Networks

OBJEKTIF

Kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat hendaklah diasingkan dalam rangkaian organisasi.

KETERANGAN	TINDAKAN
a) Pengasingan rangkaian hendaklah dibuat mengikut kesesuaian dan keperluan persekitaran jabatan/agensi. b) Pengasingan rangkaian hendaklah dikaji, dirancang dan dilaksanakan.	Pentadbir Sistem Operasi

8.23 TAPISAN LAMAN WEB

Web Filtering

OBJEKTIF

Akses kepada laman web luaran hendaklah diuruskan untuk mengurangkan pendedahan kepada kandungan berniat jahat.

KETERANGAN	TINDAKAN
Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang warga kerja daripada mengakses laman web luaran yang mungkin mengandungi virus, bahan yang tidak selamat, data atau jenis maklumat haram yang lain dengan: a) Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah. Pekeliling	ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 atau pekeliling-peliling semasa; b) Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat; c) Laman Web yang mengandungi kefungsian *Command-and-Control Server;* d) Laman web berniat jahat yang diperoleh daripada *scammer*; dan e) Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	

8.24 PERATURAN KAWALAN KRIPTOGRAFI

Regulation of Cryptographic Controls

OBJEKTIF

Peraturan untuk penggunaan kriptografi yang berkesan, termasuk kunci kriptografi pengurusan, hendaklah ditakrifkan dan dilaksanakan.

KETERANGAN	TINDAKAN
Kawalan kriptografi hendaklah dilaksanakan mengikut keperluan perundangan dan peraturan-peraturan yang berkuat kuasa.	ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna

8.25 DASAR KESELAMATAN PEMBANGUNAN

Secure Development Policy

OBJEKTIF

Peraturan untuk pembangunan perisian dan sistem yang selamat hendaklah ditubuhkan dan dilaksanakan.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Keselamatan persekitaran pembangunan; b) Keselamatan pangkalan data; c) Keselamatan *source code*; d) Keselamatan data dan maklumat; e) Keselamatan dalam kawalan versi; dan f) Pengaturcaraan secara selamat.	ICTSO Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi

8.26 ANALISIS KEPERLUAN DAN SPESIFIKASI KESELAMATAN MAKLUMAT

Information Security Requirement Analysis and Spesification

OBJEKTIF

Keperluan keselamatan maklumat hendaklah dikenal pasti, dinyatakan dan diluluskan semasa membangunkan atau memperoleh permohonan.

KETERANGAN	TINDAKAN
Keperluan keselamatan maklumat bagi pembangunan sistem aplikasi baharu dan penambahbaikan sistem aplikasi hendaklah mematuhi perkara-perkara berikut:	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi

KETERANGAN	TINDAKAN
a) Semua sistem aplikasi yang dibangunkan hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS; b) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem aplikasi hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; c) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem aplikasi bagi memastikan kesahihan dan integriti data; dan d) Merancang penilaian tahap keselamatan sistem aplikasi sebelum sistem aplikasi baharu diguna pakai.	

8.27 KESELAMATAN PRINSIP KEJURUTERAAN SISTEM

Secure System Engineering Principle

OBJEKTIF

Maklumat aktiviti bagi prinsip untuk keselamatan sistem kejuruteraan hendaklah diwujudkan, didokumenkan, diselenggara dan digunakan untuk sebarang pembangunan sistem.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Prosedur hendaklah diwujudkan, didokumentasi, diselenggara dan diguna pakai dalam pelaksanaan	Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi

KETERANGAN	TINDAKAN
pembangunan sistem aplikasi berdasarkan prinsip kejuruteraan yang selamat; b) Merancang penyediaan sistem aplikasi baharu berdasarkan Garis Panduan Pembangunan Aplikasi (KRISA); c) Keselamatan perlu diambil kira dalam semua peringkat pembangunan sistem aplikasi; dan d) Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa.	

8.28 PENGEKODAN SELAMAT

Secure Coding

OBJEKTIF

Prinsip pengekodan selamat hendaklah digunakan untuk pembangunan perisian.

KETERANGAN	TINDAKAN
Amalan dan prosedur pengekodan yang selamat hendaklah mengambilkira perkara berikut untuk proses pengekodan: a) Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan;	ICTSO Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi

KETERANGAN	TINDAKAN
b) Penggunaan teknik dan kaedah pengaturcaraan selamat seperti pembangunan sistem aplikasi yang hendak dilakukan disarankan dibuat pengujian dan *pair programming*; c) Penggunaan kaedah pengaturcaraan yang berstruktur; d) Dokumentasi kod sumber yang betul dan penyingkiran kecacatan kod sumber; e) Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod sumber yang tidak diluluskan atau kata laluan berkod keras (*hard code*); dan f) Kod sumber yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	

8.29 PENGUJIAN KESELAMATAN SISTEM

System Security Testing

OBJEKTIF

Proses ujian keselamatan sistem hendaklah ditakrifkan dan dilaksanakan dalam kitaran hayat pembangunan.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut:	Pemilik Sistem ICT Pembangun Sistem ICT

KETERANGAN	TINDAKAN
a) Semua sistem aplikasi baharu dan penambahbaikan sistem hendaklah menjalani ujian dan pengesahan fungsi keselamatan; b) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam sistem aplikasi bagi menjamin proses dan ketepatan maklumat; c) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam sistem aplikasi; d) Membuat semakan pengesahan di dalam sistem aplikasi untuk mengenal pasti sebarang pencemaran maklumat; e) Menjalankan proses semak ke atas *ouput* data daripada setiap proses sistem untuk menjamin ketepatan dan kesesuaian; dan f) Melaksanakan ujian penembusan sistem aplikasi secara luaran dan dalaman oleh pihak yang bertauliah dalam keselamatan sistem.	Pentadbir Sistem Aplikasi

8.30 PEMBANGUNAN SISTEM SUMBER LUAR

Outsourced System Development

OBJEKTIF

Organisasi hendaklah mengarah, memantau dan menyemak aktiviti yang berkaitan pembangunan sistem secara penyumberan luar.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Hak harta intelek, *source code* dan data bagi sistem aplikasi yang dibangunkan adalah menjadi hak milik Kerajaan Negeri Johor; b) Keperluan perjanjian hendaklah merangkumi amalan reka bentuk, pengaturcaraan dan pengujian yang selamat; c) Mengenal pasti risiko dan menentukan tahap kawalan keselamatan; d) Spesifikasi perolehan hendaklah mengandungi klausa berhubung keperluan keselamatan, ketersediaan kod sumber, keperluan integrasi, keperluan pelupusan data, keperluan migrasi data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan; dan e) Pihak ketiga hendaklah menjalani tapisan keselamatan sebelum memulakan kerja-kerja pembangunan sistem.	ICTSO Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi Pembekal

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI

Separation of Development, Test and Operational Facilities

OBJEKTIF

Persekitaran pembangunan, ujian dan pengeluaran hendaklah diasingkan dan terjamin.

KETERANGAN	TINDAKAN
Persekitaran bagi pembangunan dan pengujian sistem aplikasi hendaklah diasingkan dari persekitaran yang digunakan untuk pengoperasian.	Pentadbir Sistem ICT

8.32 PENGURUSAN PERUBAHAN

Change Management

OBJEKTIF

Perubahan kepada kemudahan pemprosesan maklumat dan sistem maklumat hendaklah tertakluk kepada prosedur pengurusan perubahan.

KETERANGAN	TINDAKAN
a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Ketua Jabatan / pemilik aset ICT; b) Pemasangan, penyelenggaraan, penghapusan dan pengemaskinian pada komponen aset ICT hendaklah dikendalikan oleh pengguna atau pembekal yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Pengubahsuaian komponen aset ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; d) Perubahan atau pengubahsuaian hendaklah diuji, direkod dan dikawal bagi mengelakkan berlakunya ralat; dan	Ketua Jabatan / Agensi Pentadbir Sistem ICT Pengguna

KETERANGAN	TINDAKAN
e) Ralat yang dikenal pasti hendaklah dibuat pengolahan dan disahkan sebelum diguna pakai.	

8.33 PERLINDUNGAN DATA UJIAN

Protection of Test Data

OBJEKTIF

Maklumat ujian hendaklah dipilih, dilindungi dan diurus dengan sewajarnya.

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Data dan *source code* yang hendak diuji perlu dipilih, dilindungi dan dikawal; b) Hanya data yang diperlukan untuk tujuan pengujian sahaja digunakan; c) Pengujian hendaklah dibuat ke atas *source code* yang terkini; dan d) Mengaktifkan log audit bagi merekod aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem Aplikasi

8.34 KAWALAN AUDIT SISTEM MAKLUMAT

Information Systems Audit Control

OBJEKTIF

Ujian audit dan aktiviti jaminan lain yang melibatkan penilaian sistem operasi hendaklah dirancang dan dipersetujui antara penguji dan pengurusan yang sesuai.

KETERANGAN	TINDAKAN
a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas operasi sistem hendaklah dirancang dan dipersetujui oleh ICTSO untuk meminimumkan gangguan dalam sistem penyampaian perkhidmatan; dan b) Laporan audit ICT perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO Pengurus ICT Pentadbir Sistem ICT

GLOSARI

GLOSARI

ISTILAH	KETERANGAN
ANCAMAN	Sesuatu yang boleh menyebabkan bahaya, kerosakan dan kerugian.
ANTIVIRUS	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CD-ROM untuk sebarang kemungkinan adanya virus.
ASET ICT	Maklumat, aliran data, sistem, platform sistem & perisian, perkakasan fizikal, manusia dan sumber luaran.
CHECKS-AND-BALANCES	Mengimbangi pengaruh yang mana organisasi atau sistem dikawalselia, biasanya mereka yang memastikan bahawa kuasa organisasi tidak tertumpu di tangan individu atau kumpulan.
CDO	Personel yang dilantik dan bertanggungjawab terhadap aset ICT bagi menyokong hala tuju ICT Kerajaan Negeri Johor.
CLEAR DESK	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
CLEAR SCREEN	Tidak meninggalkan paparan di skrin apabila pengguna tidak berada di tempatnya.
ENKRIPSI	Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
FAIL LOG	Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut: Fail log sistem pengoperasian; Fail log servis (Contoh: web, e-mel); Fail log aplikasi; dan Fail log rangkaian (Contoh: *switch, firewall, IPS*).

ISTILAH	KETERANGAN
FIREWALL	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya
IMPAK FUNGSI	Impak fungsi jabatan/agensi melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.
IMPAK TEKNIKAL	Impak teknikal melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
INSIDEN KESELAMATAN	Musibah yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
INTEGRITI	Data dan maklumat yang hanya boleh diubah dengan cara yang dibenarkan.
IPS	Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan. Contoh: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
KERAHSIAAN	Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran
KERAJAAN NEGERI JOHOR	Merangkumi semua jabatan/agensi di bawah Pentadbiran Kerajaan Negeri Johor termasuk Badan Berkanun Negeri dan Pihak Berkuasa Tempatan.
KERENTANAN *VULNERABILITY*	Kelemahan atau kecacatan aset yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
KESELAMATAN	Keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima.
KESELAMATAN ICT	Keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan.

ISTILAH	KETERANGAN
KETERSEDIAAN	Data dan maklumat yang boleh dicapai pada bila-bila masa.
KRIPTOGRAFI	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
MAKLUMAT RAHSIA RASMI	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 2B Akta Rahsia Rasmi 1972.
MEDIA STORAN	Peranti atau bahan yang digunakan untuk menyimpan data atau maklumat secara digital. Jenis media storan yang digunakan Cakera Keras (*Hard Disk Drives, HDD*), Cakera Keadaan Pepejal (*Solid State Drives, SSD*), Pemacu Kilat USB (*USB Flash Drive*) dan Storan Awan (*Cloud Storage*).
MEREKAYASA REENGINEERING	Mengemaskini, merekabentuk semula dan menambah nilai
PEGAWAI PENGELAS	Personel yang bertanggungjawab menguruskan dokumen Rahsia Rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuatkuasa.
PEGAWAI ASET	Pegawai aset memainkan peranan penting dalam memastikan bahawa aset organisasi diurus dengan baik, yang boleh membantu mengurangkan kos, meningkatkan kecekapan operasi, dan memaksimumkan nilai aset tersebut.
PEMALSUAN	Penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat dan penipuan.
PEMBANGUN SISTEM ICT	Pihak yang membangunkan sistem yang berkaitan

ISTILAH	KETERANGAN
PEMBEKAL	Pihak yang menyediakan sesuatu perkhidmatan atau produk.
PEMILIK SISTEM ICT	Jabatan/Agensi yang empunya sistem berkaitan
PENGESAHAN *AUTHENTICATION*	Kaedah untuk mengesahkan identiti pengguna, peralatan atau entiti dalam sistem komputer sebelum kebenaran capaian kepada sesuatu sistem diberikan.
PENGGUNA	Pihak yang menggunakan perkhidmatan atau produk yang berkaitan.
PENGOLAHAN RISIKO	Proses memilih dan melaksanakan tindakan untuk mengelak, mengurang, menerima atau memindah risiko dengan mengambil kira kos dan faedah.
PENILAIAN RISIKO	Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
PENTADBIR SISTEM ICT	Merupakan pentadbir sistem operasi dan pentadbir sistem aplikasi.
PERISIAN	Merujuk kepada pakej aplikasi yang digunakan.
PERSONEL	Pegawai atau kakitangan Kerajaan Negeri Johor termasuk Badan Berkanun Negeri dan Pihak Berkuasa Tempatan.
PKI	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
RESTORE	Pemulihan
RISIKO	Kebarangkalian dan impak sesuatu insiden berlaku berpunca daripada kerentanan atau ancaman yang dikenalpasti.
SANDARAN BACKUP	Salinan

ISTILAH	KETERANGAN
SISTEM LUARAN	Sistem yang dibangunkan oleh sumber luar di bawah Kerajaan Negeri Johor yang dihubungkan dengan sistem jabatan/agensi.
SUMBER LUAR OUTSOURCE	Perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
SISTEM	Merujuk kepada sistem aplikasi.
TANPA SANGKALAN	Punca maklumat hendaklah daripada sumber yang sah dan tidak boleh dinafikan sistem.
UPS	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
USER END POINT DEVICES	Peranti akhir pengguna merujuk kepada peralatan atau peranti yang digunakan untuk menyimpan, mengakses dan berinteraksi dengan rangkaian atau sistem. Contoh peranti akhir pengguna termasuk komputer, komputer riba, telefon pintar, tablet dan sebarang peralatan digunakan untuk menyimpan, mengakses dan berinteraksi dengan rangkaian atau sistem.
KEISTIMEWAAN UTILITI	Aplikasi yang memerlukan capaian istimewa untuk berfungsi. Contoh: perisian antivirus.
UTILITI SOKONGAN	Peralatan atau program yang membantu kelancaran fungsi aset ICT seperti UPS, set janakuasa dan antivirus.
KOORDINATOR PKP	Bertanggungjawab merancang, menyelaras, menguji, dan memperbaiki pelan kesinambungan untuk memastikan kelangsungan operasi kritikal organisasi dalam menghadapi risiko dan gangguan.

SENARAI PERUNDANGAN DAN PERATURAN-PERATURAN

SENARAI PERUNDANGAN DAN PERATURAN - PERATURAN

BIL	SENARAI PERATURAN
1	Arahan Keselamatan (Semakan dan Pindaan 2017).
2	Arahan MKN No. 20 (Semakan Semula) - Dasar dan Mekanisme Pengurusan Bencana Negara
3	Arahan MKN No. 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara
4	Pekeliling Am Bil.1 Tahun 2015 - Pelaksanaan Data Terbuka Sektor Awam
5	Rancangan Malaysia ke - 12
6	Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam
7	Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam - 25 Januari 2015 Digital Document Management System 2.0 (DDMS 2.0)
8	Dasar Kriptografi Negara - 12 Julai 2013
9	Pekeliling Perbendaharaan Malaysia PK 2 (setakat Jun 2024) - Kaedah Perolehan Kerajaan
10	Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia
11	Pegawai Keselamatan Kerajaan 5 Jun 2012 - Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam (Pindaan Kedua)
12	PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2022
13	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat - 24 November 2010

BIL	SENARAI PERATURAN
14	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat - 24 November 2010
15	Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam - 22 Januari 2010
16	Akta 709 - Akta Perlindungan Data Peribadi 2010
17	Surat Pekeliling Am Bil.3 Tahun 2009 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam
18	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan - 23 November 2007
19	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan - 1 Jun 2007
20	Arahan Teknologi Maklumat, MAMPU, 2007
21	Akta 680 - Aktiviti Kerajaan Elektronik 2007
22	Arahan Ketua Setiausaha Negara Bil.1 Tahun 2007 - Langkah-Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-Lain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensi-Agensi Kerajaan
23	Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan - 20 Oktober 2006
24	Surat Pekeliling Am Bil.4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
25	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006

BIL	SENARAI PERATURAN
26	Akta 658 - Akta Perdagangan Elektronik 2006
27	Surat Pekeliling Am Bil.6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
28	Akta 629 - Akta Arkib Negara 2003 - Seksyen 27(1) Dan (3) Jadual Pelupusan Rekod
29	Akta 606 - Akta Cakera Optik 2000
30	Akta 588 - Akta Komunikasi dan Multimedia 1998
31	Akta 562 - AktaTandatangan Digital 1997
32	Akta 563 - Akta Jenayah Komputer 1997
33	Akta 564 - Telemedicine Act 1997
34	Akta 88 - Akta Rahsia Rasmi 1972
35	Akta 332 - Akta Hak Cipta 1987
36	Surat Pekeliling Am Bil.2/1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987)
37	Akta 298 - Kawasan Larangan Tempat Larangan 1959 Akta 56 - Akta Keterangan 1950
38	National Cyber Security Policy (NCSP)
30	Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisations
40	Arahan Tetap Sasaran Penting

BIL	SENARAI PERATURAN
41	Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara
42	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi
43	Perintah Am Bab D
45	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
46	Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan
47	Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT).
48	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-Agensi Kerajaan
49	Surat Pekeliling Am Bil 2 Tahun 2000 – Peranan Jawatankuasa-Jawatankuasa Di Bawah Jawatankuasa IT & Internet Kerajaan (JITIK)
50	Surat Pekeliling Am Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Bil 1 Tahun 2016 – Tatacara Pelaksanaan Projek ICT Di Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO)
51	Surat Pekeliling Am Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Bil 2 Tahun 2016 – Garis Panduan Kesediaan Infrastruktur Teknologi Maklumat Dan Komunikasi (ICT) Di Agensi & Fasiliti Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO)
52	Malaysia Public Sector Management of Information and Communications Technology Security Handbooks (MyMIS) 2002
53	Surat Akuan Ketua Pengarah MAMPU Tahun 2009 – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-Agensi Kerajaan
54	Surat Arahan Ketua Pengarah MAMPU Tahun 2010 – Pemantapan Penggunaan Dan Pengurusan Emel Di Agensi-Agensi Kerajaan
55	Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA) yang bertarikh 28 Januari 2019.

BIL	SENARAI PERATURAN
56	Garis Panduan Keselamatan MAMPU 2004
57	Standard Operating Procedure (SOP) ICT
58	Arahan Perbendaharaan
59	Akta Keselamatan Siber 2024

SURAT AKUAN PEMATUHAN

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER KERAJAAN NEGERI JOHOR

NAMA (HURUF BESAR) : _____

NO. KAD PENGENALAN : _____

JAWATAN : _____

BAHAGIAN : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam **POLISI KESELAMATAN SIBER KERAJAAN NEGERI JOHOR VERSI 1.0;** dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN :
TARIKH :

DISAHKAN OLEH :
[KETUA PEGAWAI DIGITAL (CDO)]
TARIKH :

ICT@Johor
Aras 1,
Bangunan Dato' Jaafar Muhammad,
Kota Iskandar, 79503 Iskandar Puteri,
Johor, Malaysia
607 266 6660