DKICT 2.0

DASAR KESELAMATAN ICT KERAJAAN NEGERI JOHOR
VERSI 2.0

NOVEMBER 2017

KANDUNGAN

A. SEJARAH DOKUMEN

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

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)

C. KELULUSAN DOKUMEN

BAGI PIHAK SUK KERAJAAN NEGERI JOHOR
DISEDIAKAN OLEH : ..... NAMA : YBM TUNKU ZAHRAH BINTI TUNKU OSMAN JAWATAN : ICTSO NEGERI JOHOR TARIKH : 5/4/2018
DISAHKAN OLEH : ..... NAMA : DR. HAJI BADRUL HISHAM BIN KASSIM JAWATAN : CIO NEGERI JOHOR TARIKH : 5/4/218
DILULUSKAN OLEH : ..... NAMA : DATO' HAJI AZMI BIN ROHANI JAWATAN : SETIAUSAHA KERAJAAN JOHOR TARIKH : 5/4/2018

D. SINGKATAN

ISTILAH	KETERANGAN / TAKRIFAN
CIO	*Chief Information Officer* Ketua Pegawai Maklumat
DKICT	Dasar Keselamatan ICT Kerajaan Negeri Johor
GCERT	*Government Computer Emergency 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*
Johor CERT	*Johor Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Negeri Johor
JPICT	Jawatankuasa Pemandu ICT Negeri Johor
LAN	*Local Area Network* Rangkaian Kawasan Setempat
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
PKI	*Public Key Infrastructure* Infrastruktur Kekunci Awam
PKP	Pelan Kesinambungan Perkhidmatan
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
SLA	*Service Level Agreement* Perjanjian Tahap Perkhidmatan
SLG	*Service Level Guarantee* Jaminan Tahap Perkhidmatan
UPS	*Uninterruptable Power Supply* Bekalan Kuasa Berterusan

1.0 PENGENALAN

DKICT ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam penggunaan 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

DKICT ini bertujuan untuk menerangkan tanggungjawab dan peranan pengguna dan pembekal.

3.0 OBJEKTIF

Objektif utama DKICT ini adalah seperti berikut:

a) Memastikan kelancaran operasi Kerajaan Negeri Johor dan meminimumkan kerosakan atau kemusnahan;

b) Melindungi kepentingan pengguna dan pembekal dari kesan kegagalan atau kerentanan aset ICT; dan

c) Melindungi aset ICT Kerajaan Negeri Johor daripada sebarang ancaman.

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.

DKICT 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

DKICT 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 mengurangkan risiko.

(ii) PROSES

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

- Proses
- *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 sekurang-kurangnya dua kali setahun dalam Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Negeri Johor.

BIDANG 1

DASAR KESELAMATAN MAKLUMAT
Information Security Policy

1.1 HALA TUJU PENGURUSAN KE ATAS KESELAMATAN MAKLUMAT
Management Direction 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 DKICT ini akan dijalankan oleh Setiausaha Kerajaan Johor dengan disokong oleh JPICT yang terdiri daripada CIO, ICTSO dan ahli-ahli yang dilantik oleh Setiausaha Kerajaan Johor. DKICT hendaklah dipatuhi oleh semua pengguna dan pembekal.	Setiausaha Kerajaan Johor Pengguna Pembekal

1.1.1 DASAR KESELAMATAN MAKLUMAT
Policies for Information Security

KETERANGAN	TINDAKAN
Dasar-dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan Kerajaan Negeri Johor kepada pengguna dan pembekal.	ICTSO Negeri

1.1.2 KAJIAN SEMULA DASAR KESELAMATAN MAKLUMAT

Review of Policies for Information Security

KETERANGAN	TINDAKAN
DKICT ini perlu dikaji semula secara berkala atau apabila berlaku perubahan kepada aplikasi, prosedur, perundangan dan dasar Kerajaan.	ICTSO Negeri ICTSO Jabatan/Agensi
Berikut adalah prosedur yang berhubung dengan kajian semula DKICT: 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) DKICT ini hendaklah dikaji semula mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	JPICT

BIDANG 2

ORGANISASI KESELAMATAN MAKLUMAT
Organization of Information Security

2.1 STRUKTUR ORGANISASI KESELAMATAN KERAJAAN NEGERI JOHOR
Internal Organization

OBJEKTIF

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

KETERANGAN	TINDAKAN
SETIAUSAHA KERAJAAN JOHOR Peranan dan tanggungjawab Setiausaha Kerajaan Johor adalah seperti berikut: a) Menguatkuasakan pelaksanaan DKICT; b) Memastikan pengguna dan pembekal memahami dan mematuhi peruntukan-peruntukan di bawah DKICT; 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 DKICT; dan e) Melantik CIO Negeri Johor dan ICTSO Negeri Johor serta memaklumkan pelantikan kepada Ketua Pengarah MAMPU.	Setiausaha Kerajaan Johor

KETERANGAN	TINDAKAN
KETUA JABATAN/AGENSI Peranan dan tanggungjawab adalah seperti berikut: a) Memastikan pengguna dan pembekal memahami dan mematuhi peruntukan-peruntukan di bawah DKICT; b) Memastikan semua keperluan organisasi seperti sumber kewangan, personel dan perlindungan keselamatan maklumat adalah mencukupi; c) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT; dan d) Melantik CIO Jabatan/Agensi, ICTSO Jabatan/Agensi dan Pengurus ICT serta memaklumkan pelantikan kepada ICTSO Negeri Johor.	Ketua Jabatan/Agensi
CIO NEGERI JOHOR Peranan dan tanggungjawab CIO Negeri Johor adalah seperti berikut: a) Membantu Setiausaha Kerajaan Johor dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; c) Memastikan Pelan Strategik ICT Kerajaan Negeri Johor mengandungi aspek keselamatan ICT; dan	CIO Negeri Johor

KETERANGAN	TINDAKAN
d) 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 DKICT; 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 menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan ICT kepada GCERT dan seterusnya membantu dalam penyiasatan atau pemulihan; e) Melaporkan insiden keselamatan ICT kepada CIO 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;	ICTSO Negeri Johor

KETERANGAN	TINDAKAN
g) Melaksanakan pematuhan DKICT 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.	
CIO Jabatan/Agensi Peranan dan tanggungjawab CIO Jabatan/Agensi adalah seperti berikut: a) Membantu Ketua Jabatan/Agensi dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; c) Memastikan Pelan Strategik ICT Jabatan/Agensi mengandungi aspek keselamatan ICT; dan d) Menyelaras pelan latihan dan program kesedaran keselamatan ICT.	CIO Jabatan/Agensi
ICTSO Jabatan/Agensi Peranan dan tanggungjawab ICTSO Jabatan/Agensi yang dilantik adalah seperti berikut: a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT;	ICTSO Jabatan/Agensi

KETERANGAN	TINDAKAN
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 menyediakan langkah-langkah perlindungan yang bersesuaian; d) Melaporkan insiden keselamatan ICT kepada Johor CERT dan seterusnya membantu dalam penyiasatan atau pemulihan; e) Melaporkan insiden keselamatan ICT kepada CIO Jabatan/Agensi bagi insiden yang memerlukan pengaktifan PKP; e) 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 DKICT 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.	

KETERANGAN	TINDAKAN
PENGURUS ICT Peranan dan tanggungjawab Pengurus ICT adalah melaksanakan keperluan DKICT dalam operasi semasa seperti berikut: a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan 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.	Pengurus ICT
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 DKICT; c) Memantau aktiviti capaian harian sistem ICT;	Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e) Menganalisis dan menyimpan rekod jejak audit; f) 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. **JOHOR CERT** Peranan dan tanggungjawab Johor CERT 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;	JPICT Johor CERT

KETERANGAN	TINDAKAN
c) Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Mengesyorkan Kerajaan Negeri Johor untuk mengambil 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 DKICT; 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 DKICT dan menjaga kerahsiaan maklumat Kerajaan Negeri Johor; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;	Pengguna

KETERANGAN	TINDAKAN
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; 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 DKICT.	

BIDANG 3

KESELAMATAN SUMBER MANUSIA
Human Resource Security

3.1 SEBELUM PERKHIDMATAN
Prior to Employment

OBJEKTIF

Memastikan pengguna dan pembekal memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan ICT.

3.1.1 TAPISAN KESELAMATAN
Screening

KETERANGAN	TINDAKAN
Menjalankan tapisan keselamatan terhadap pengguna dan pembekal yang terlibat selaras dengan keperluan perkhidmatan.	Setiausaha Kerajaan Johor Ketua Jabatan

3.1.2 TERMA DAN SYARAT PERKHIDMATAN
Terms and Conditions of Employment

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.	

3.2 DALAM PERKHIDMATAN

During Deployment

OBJEKTIF

Memastikan pengguna dan pembekal mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pihak yang terlibat hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

3.2.1 TANGGUNGJAWAB PENGURUSAN

Management Responsibilities

KETERANGAN	TINDAKAN
a) Memastikan pengguna dan pembekal memahami dan mematuhi perundangan, Arahan Perkhidmatan, peraturan dan DKICT; dan b) Memastikan pengguna dan pembekal mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh Kerajaan Negeri Johor.	Pengguna Pembekal

3.2.2 LATIHAN, PENDIDIKAN DAN KESEDARAN KESELAMATAN MAKLUMAT

Information Security Awareness, Education and Training

KETERANGAN	TINDAKAN
Program kesedaran mengenai keselamatan maklumat secara berterusan hendaklah diberikan dalam melaksanakan tugas-tugas dan tanggungjawab.	Pengguna Pembekal

3.2.3 PROSES TATATERTIB

Disciplinary Process

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

3.3 PENAMATAN ATAU PERTUKARAN PERKHIDMATAN

Termination or Change of Employment

OBJEKTIF

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

3.3.1 TANGGUNGJAWAB APABILA PENAMATAN ATAU PERTUKARAN PERKHIDMATAN

Termination or Change of Employment Responsibilities

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

BIDANG 4

PENGURUSAN ASET
Asset Management

4.1 TANGGUNGJAWAB TERHADAP ASET
Responsibility for Asset

OBJEKTIF

Mengenal pasti aset ICT dan menentukan tanggungjawab perlindungan yang bersesuaian.

4.1.1 INVENTORI ASET
Inventory of Asset

KETERANGAN	TINDAKAN
Tanggungjawab yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa. 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 Personel

4.1.2 PENEMPATAN ASET

Ownership of Asset

KETERANGAN	TINDAKAN
Semua personel adalah bertanggungjawab ke atas aset ICT di bawah kawalannya. Semua aset ICT yang ditempatkan hendaklah diuruskan dengan baik oleh personel.	Pegawai Aset Personel

4.1.3 PENERIMAAN PENGGUNAAN ASET

Acceptable Use of Asset

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

4.1.4 PEMULANGAN ASET

Return of Asset

KETERANGAN	TINDAKAN
Memastikan semua aset ICT dikembalikan kepada jabatan/agensi mengikut peraturan dan terma perkhidmatan yang ditetapkan.	Pegawai Aset Personel

4.2 KLASIFIKASI MAKLUMAT

Information Classification

OBJEKTIF

Memastikan aset ICT diberikan tahap perlindungan yang bersesuaian.

4.2.1 PENGELASAN MAKLUMAT

Classification of Information

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

4.2.2 PELABELAN MAKLUMAT

Labelling of Information

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

4.2.3 PENGENDALIAN ASET

Handling of Asset

KETERANGAN	TINDAKAN
Aktiviti pengendalian maklumat hendaklah mengambil kira langkah-langkah keselamatan berikut:	Pentadbir Sistem ICT Personel

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 dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada Maklumat Rahsia Rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Melindungi kerahsiaan aset ICT dari diketahui umum.	

4.3 PENGENDALIAN MEDIA

Media handling

OBJEKTIF

Melindungi maklumat dalam media storan dari sebarang pendedahan, pengubahsuaian, pemindahan dan pemusnahan.

4.3.1 PENGURUSAN MEDIA MUDAH ALIH

Management of Removable Media

KETERANGAN	TINDAKAN
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a) Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut Arahan Keselamatan; b) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; c) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; d) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; e) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan f) Menyimpan semua media di tempat yang selamat.	ICTSO Pengurus ICT Pentadbir Sistem ICT

4.3.2 PELUPUSAN MEDIA

Disposal of Media

KETERANGAN	TINDAKAN
Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT.	ICTSO Pengurus ICT

KETERANGAN	TINDAKAN
Media yang mengandungi Maklumat Rahsia Rasmi yang perlu dihapuskan atau dimusnahkan hendaklah mengikut prosedur yang betul.	Personel

4.3.3 PEMINDAHAN MEDIA FIZIKAL

Physical Media Transfer

KETERANGAN	TINDAKAN
Memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan.	ICTSO Pengurus ICT Personel

BIDANG 5

KAWALAN CAPAIAN
Access Control

5.1 KEPERLUAN KAWALAN CAPAIAN PERKHIDMATAN
Business requirement of access control

OBJEKTIF

Menghadkan capaian kepada maklumat dan kemudahan pemprosesan maklumat.

5.1.1 DASAR KAWALAN CAPAIAN
Access Control Policy

KETERANGAN	TINDAKAN
Prosedur kawalan capaian hendaklah diwujudkan, didokumenkan, 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;	ICTSO Pengurus ICT Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
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.	

5.1.2 CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN

Access to Network and Network Services

KETERANGAN	TINDAKAN
Capaian ke rangkaian dan perkhidmatan rangkaian hendaklah mendapat kebenaran. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Menghadkan capaian di antara rangkaian Kerajaan Negeri Johor, rangkaian agensi lain dan rangkaian awam; dan b) Memantau dan menguatkuasakan kawalan capaian terhadap perkhidmatan rangkaian ICT.	ICTSO Pengurus ICT Pentadbir Sistem (Operasi)

5.2 PENGURUSAN CAPAIAN PENGGUNA

User Access Management

OBJEKTIF

Menguruskan capaian pengguna terhadap sistem dan perkhidmatan.

5.2.1 PENGURUSAN PENGGUNA

User Registration and De-registration

KETERANGAN	TINDAKAN
Prosedur Pengurusan Pengguna hendaklah diwujudkan dan dilaksanakan untuk membolehkan hak capaian diuruskan.	ICTSO Pengurus ICT Pentadbir Sistem ICT

5.2.2 PENGURUSAN HAK CAPAIAN *PRIVILEGE*

Management of Privileged Access Rights

KETERANGAN	TINDAKAN
Penetapan dan penggunaan ke atas hak capaian *privilege* hendaklah dikawal selia, dipantau dan dikemaskini.	Pengurus ICT

5.2.3 PENGURUSAN HAK CAPAIAN

Removal or Adjustment of Access Rights

KETERANGAN	TINDAKAN
Prosedur hendaklah diwujudkan dan dilaksanakan untuk menguruskan hak capaian pengguna ke atas sistem dan perkhidmatan.	ICTSO Pengurus ICT
Pengesahan tahap capaian yang diberikan hendaklah sesuai dengan Dasar Kawalan Capaian (Rujuk 5.1.1).	Pentadbir Sistem ICT

5.3 TANGGUNGJAWAB PENGGUNA

User Responsibilities

OBJEKTIF

Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan diri.

5.3.1 PENGGUNAAN KATA LALUAN

Use of Secret Authentication Information

KETERANGAN	TINDAKAN
Pengguna hendaklah mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan untuk melindungi maklumat yang digunakan sebagai pengesahan diri.	Pengguna

5.4 KAWALAN CAPAIAN SISTEM

System Access Control

OBJEKTIF

Menghalang capaian yang tidak dibenarkan kepada sistem.

5.4.1 SEKATAN CAPAIAN MAKLUMAT

Information Access Restriction

KETERANGAN	TINDAKAN
Capaian kepada fungsi maklumat dan sistem hendaklah dihadkan mengikut Dasar Kawalan Capaian (Rujuk 5.1.1). Capaian maklumat terhad kepada pengguna dan tujuan yang dibenarkan.	Pentadbir Sistem ICT Pengguna

5.4.2 PROSEDUR LOG MASUK

Secure Log - On Procedure

KETERANGAN	TINDAKAN
Setiap aktiviti capaian sistem maklumat pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini. Prosedur Log Masuk hendaklah diwujudkan dan dilaksanakan.	Pentadbir Sistem ICT

5.4.3 PENGURUSAN KATA LALUAN

Password Management

KETERANGAN	TINDAKAN
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem hendaklah mengikut amalan terbaik.	Pengguna

5.4.4 PENGGUNAAN PROGRAM UTILITI *PRIVILEGE*

Use of Privileged Utility Programs

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

5.4.5 KAWALAN CAPAIAN KEPADA *SOURCE CODE*

Access Control to Program Source Code

KETERANGAN	TINDAKAN
Capaian kepada *source code* hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan seperti berikut: a) Log audit hendaklah dikekalkan kepada semua capaian *source code*;	ICTSO Pengurus ICT Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
b) Penyelenggaraan dan penyalinan *source code* hendaklah tertakluk kepada kawalan perubahan; dan c) *Source code* bagi semua sistem dan perisian aplikasi hendaklah menjadi hakmilik Kerajaan Negeri Johor.	

BIDANG 6

KRIPTOGRAFI
Cryptography

6.1 KAWALAN KRIPTOGRAFI
Cryptography Control

OBJEKTIF

Memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat.

6.1.1 DASAR PENGGUNAAN KAWALAN KRIPTOGRAFI
Policy on the Use of Cryptographic Control

KETERANGAN	TINDAKAN
Prosedur kawalan kriptografi untuk melindungi maklumat hendaklah diwujudkan dan dilaksanakan. Perkara - perkara berikut perlu dipertimbangkan: a) Pendekatan pengurusan bagi kawalan kriptografi hendaklah dilindungi; b) Tahap perlindungan hendaklah dikenal pasti berdasarkan penemuan penilaian risiko; c) Pemindahan maklumat secara mudah-alih dan merentasi talian komunikasi hendaklah menggunakan kaedah enkripsi; d) Kunci kriptografi hendaklah diuruskan dengan baik;	ICTSO Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
e) Kaedah kriptografi yang digunakan hendaklah mematuhi dasar dan peraturan yang berkuat kuasa; dan f) Implikasi penggunaan kriptografi terhadap proses yang bergantung kepada pemeriksaan kandungan.	

6.1.2 PENGURUSAN *PKI*

Public Key Infrastructure

KETERANGAN	TINDAKAN
Prosedur tentang penggunaan perlindungan dan hayat kekunci kriptografi hendaklah diwujudkan dan dilaksanakan sepanjang kitar hayatnya. Prosedur yang diwujudkan hendaklah mematuhi dasar dan peraturan yang berkuat kuasa.	ICTSO Pengurus ICT

BIDANG 7

KESELAMATAN FIZIKAL DAN PERSEKITARAN
Physical and Environmental Security

7.1 KAWASAN LARANGAN
Secure Areas

OBJEKTIF

Mencegah akses fizikal tanpa kebenaran yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat jabatan/agensi.

7.1.1 LINGKUNGAN KESELAMATAN FIZIKAL
Physical Security Parameter

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.	ICTSO Pegawai Keselamatan Jabatan/Agensi

7.1.2 KAWALAN KEMASUKAN FIZIKAL

Physical Entry Control

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

7.1.3 KAWALAN PEJABAT, BILIK DAN TEMPAT OPERASI

Securing Offices, Rooms and Facilities

KETERANGAN	TINDAKAN
Kawalan fizikal bagi ruang pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan berdasarkan Arahan Keselamatan.	ICTSO Pengurus ICT Pegawai Keselamatan Jabatan/Agensi

7.1.4 PERLINDUNGAN TERHADAP ANCAMAN LUARAN DAN PERSEKITARAN

Protecting Against External and Environmental Threat

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 Penyelaras PKP Majlis Keselamatan Negara (MKN)

7.1.5 BERTUGAS DALAM KAWASAN LARANGAN

Working in Secure Area

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

7.1.6 KAWASAN PENGHANTARAN DAN PEMUNGGAHAN

Delivery and Loading Area

KETERANGAN	TINDAKAN
Kawasan penghantaran dan pemunggahan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat.	ICTSO Pegawai Keselamatan Jabatan/Agensi

7.2 KESELAMATAN ASET ICT

Equipment

OBJEKTIF

Melindungi aset ICT daripada kehilangan, kerosakan, kecurian dan penyalahgunaan serta gangguan terhadap perkhidmatan jabatan/agensi.

7.2.1 PENEMPATAN DAN PERLINDUNGAN ASET ICT

Equipment Siting and Protection

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

7.2.2 UTILITI SOKONGAN

Supporting Utility

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

7.2.3 KESELAMATAN KABEL

Cabling Security

KETERANGAN	TINDAKAN
Kabel elektrik dan kabel telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Pelan Mekanikal dan Elektrikal Pusat Data perlu disediakan.	Pengurus ICT Pentadbir Sistem (Operasi) Pegawai Keselamatan Jabatan/Agensi

7.2.4 PENYELENGGARAAN ASET ICT

Equipment Maintenance

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

7.2.5 PERGERAKAN ASET ICT

Removal of Asset

KETERANGAN	TINDAKAN
a) Aset ICT yang hendak dibawa keluar dari premis jabatan/agensi untuk tujuan rasmi, hendaklah mendapat kelulusan dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan b) Proses pergerakan aset ICT hendaklah mendapat kelulusan dan direkodkan.	Pengurus ICT Pegawai Aset

7.2.6 KESELAMATAN ASET ICT DI LUAR PREMIS

Security of Equipment Off-Premises

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

7.2.7 PELUPUSAN DAN GUNA SEMULA ASET ICT

Secure Disposal or Re-use of Equipment

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.	Pengurus ICT Pegawai Aset

7.2.8 ASET ICT TANPA PENGAWASAN

Unattended User Equipment

KETERANGAN	TINDAKAN
Aset ICT hendaklah dijaga dan dilindungi dengan mematuhi perkara-perkara berikut: a) Menamatkan sesi setelah selesai tugas; b) Log keluar sistem atau perkhidmatan rangkaian apabila tidak lagi digunakan; dan c) Lindungi aset ICT daripada penggunaan yang tidak dibenarkan.	Pengguna Pembekal

7.2.9 DASAR *CLEAR DESK* DAN *CLEAR SCREEN*

Clear Desk and Clear Screen Policy

KETERANGAN	TINDAKAN
Dasar *Clear Desk* dan *Clear Screen* hendaklah digunapakai.	Pengguna Pembekal

BIDANG 8

KESELAMATAN OPERASI
Operations Security

8.1 TANGGUNGJAWAB DAN PROSEDUR OPERASI
Operational Procedure and Responsibility

OBJEKTIF

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

8.1.1 DOKUMENTASI PROSEDUR PENGOPERASIAN
Documented Operating Procedures

KETERANGAN	TINDAKAN
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

8.1.2 PENGURUSAN PERUBAHAN

Change Management

KETERANGAN	TINDAKAN
a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada Ketua Jabatan;	Ketua Jabatan Pentadbir Sistem 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;	Pengguna
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	
e) Ralat yang dikenal pasti hendaklah dibuat pengolahan dan disahkan sebelum diguna pakai.	

8.1.3 PENGURUSAN KAPASITI

Capacity Management

KETERANGAN	TINDAKAN
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	Pengurus ICT Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
b) Keperluan kapasiti hendaklah mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko.	

8.1.4 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI

Separation of Development, Test and Operational Facilities

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

8.2 PERLINDUNGAN DARIPADA PERISIAN BERBAHAYA

Protection from Malware

OBJEKTIF

Untuk memastikan kemudahan pemprosesan maklumat dan maklumat dilindungi daripada perisian berbahaya.

8.2.1 KAWALAN TERHADAP PERISIAN BERBAHAYA

Controls Againts Malware

KETERANGAN	TINDAKAN
Tindakan berikut hendaklah dilaksanakan:	Pengurus ICT Pentadbir Sistem ICT

KETERANGAN	TINDAKAN
a) Memasang perkakasan dan perisian keselamatan untuk mengesan perisian berbahaya mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian aplikasi yang tulen, berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuat kuasa; c) Mengimbas perisian dan sistem dengan antivirus sebelum menggunakannya; d) Mengemaskini antivirus dengan definisi terkini; e) Menyemak kandungan sistem dan maklumat 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.	Pengguna Pembekal

8.3 SANDARAN

Backup

OBJEKTIF

Mencegah kehilangan maklumat.

8.3.1 SANDARAN MAKLUMAT

Information Backup

KETERANGAN	TINDAKAN
Perkara berikut hendaklah dilaksanakan bagi memastikan sistem dapat dipulihkan: a) Membuat sandaran penuh ke atas semua sistem dan perisian sekurang-kurangnya sekali dan setelah mendapat 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

8.4 LOG DAN PEMANTAUAN

Logging and Monitoring

OBJEKTIF

Merekod kronologi dan menjana fakta pembuktian.

8.4.1 LOG KRONOLOGI

Event logging

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 sekurang-kurangnya tiga (3) bulan. c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem 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 Pengurus ICT untuk tindakan selanjutnya.	Pengurus ICT Pentadbir Sistem ICT Pengguna

8.4.2 PERLINDUNGAN MAKLUMAT LOG

Protection of log information

KETERANGAN	TINDAKAN
Kemudahan merekod dan maklumat log hendaklah dilindungi.	Pentadbir Sistem ICT

8.4.3 LOG PENTADBIR DAN OPERATOR

Administrator and Operator Log

KETERANGAN	TINDAKAN
a) Pemantauan penggunaan kemudahan memproses maklumat hendaklah diwujudkan;	ICTSO
b) Hasil pemantauan perlu dilaporkan kepada ICTSO dan perlu dipantau secara berkala;	Pengurus ICT Pentadbir Sistem ICT
c) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Log hendaklah dilindungi dan jejak audit disemak dan dilapor jika perlu;	ICTSO Pengurus ICT
d) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;	Pentadbir Sistem ICT
e) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan	
f) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pengurus ICT hendaklah melaporkan kepada ICTSO.	

8.4.4 KESERAGAMAN WAKTU

Clock Synchronisation

KETERANGAN	TINDAKAN
Waktu sistem pemprosesan maklumat atau domain keselamatan hendaklah diselaraskan dengan sumber waktu yang ditetapkan oleh SIRIM.	Pentadbir Sistem ICT

8.5 KAWALAN PERISIAN OPERASI

Control of Operational Software

OBJEKTIF

Memastikan integriti perisian di dalam operasi sistem.

8.5.1 PEMASANGAN PERISIAN PADA OPERASI SISTEM

Installation of Software on Operational System

KETERANGAN	TINDAKAN
a) Pengemaskinian perisian hanya boleh dilakukan setelah mendapat kelulusan Pengurus ICT; b) Penggunaan perisian dan sistem operasi 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 Pengurus ICT; dan d) Satu strategi *rollback* harus diadakan sebelum perubahan dilaksanakan.	Pengurus ICT Pentadbir Sistem ICT

8.6 PENGURUSAN KERENTANAN TEKNIKAL

Technical Vulnerability Management

OBJEKTIF

Mengawal eksploitasi kerentanan teknikal.

8.6.1 PENGURUSAN KERENTANAN TEKNIKAL

Management of Technical Vulnerability

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Melaksanakan ujian penembusan untuk memperolehi maklumat kerentanan teknikal bagi sistem dan operasi; b) Menganalisis tahap risiko kerentanan; dan c) Mengambil tindakan pengolahan dan kawalan risiko.	Pentadbir Sistem ICT

8.6.2 KAWALAN PEMASANGAN PERISIAN

Restriction on Software Installation

KETERANGAN	TINDAKAN
a) Hanya perisian yang diperakui sahaja dibenarkan; dan b) Mengimbas perisian dan sistem dengan antivirus sebelum menggunakannya.	Pentadbir Sistem ICT Pengguna

8.7 PERTIMBANGAN AUDIT SISTEM MAKLUMAT

Information Systems Audit Consideration

OBJEKTIF

Meminimumkan kesan ke atas aktiviti audit terhadap operasi sistem.

8.7.1 KAWALAN AUDIT SISTEM MAKLUMAT

Information Systems Audit Control

KETERANGAN	TINDAKAN
Keperluan audit dan sebarang aktiviti pemeriksaan ke atas operasi sistem hendaklah dirancang dan dipersetujui oleh ICTSO untuk meminimumkan gangguan dalam sistem penyampaian perkhidmatan.	ICTSO Pengurus ICT Pentadbir Sistem ICT

BIDANG 9

KESELAMATAN KOMUNIKASI
Communications Security

9.1 PENGURUSAN KESELAMATAN RANGKAIAN
Network Security Management

OBJEKTIF

Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

9.1.1 KAWALAN RANGKAIAN
Network Control

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Memastikan kerja-kerja operasi rangkaian dilindungi; 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; d) Semua perkakasan rangkaian hendaklah mempunyai pengesahan daripada SIRIM/SKMM sebelum proses pemasangan dan konfigurasi; e) Perkakasan keselamatan rangkaian hendaklah dipasang, dikonfigurasi dan diselia;	Pengurus ICT Pentadbir Sistem (Operasi) Pengguna Pembekal

KETERANGAN	TINDAKAN
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 SLA/SLG; k) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; l) Mengawal capaian fizikal dan logikal ke atas kemudahan diagnostik dan konfigurasi jarak jauh; dan m) Mewujud dan melaksana kawalan pengalihan laluan *(routing control).*	

9.1.2 KESELAMATAN PERKHIDMATAN RANGKAIAN

Security of Network Services

KETERANGAN	TINDAKAN
Semua perkhidmatan rangkaian hendaklah mematuhi standard keselamatan yang berkuatkuasa.	Pentadbir Sistem (Operasi)

9.1.3 PENGASINGAN RANGKAIAN

Segregation in Networks

KETERANGAN	TINDAKAN
Pengasingan rangkaian hendaklah dibuat mengikut kesesuaian dan keperluan persekitaran jabatan/agensi.	Pentadbir Sistem (Operasi)

9.2 PEMINDAHAN MAKLUMAT

Information Transfer

OBJEKTIF

Memastikan pergerakan maklumat di antara jabatan/agensi dengan pembekal.

9.2.1 DASAR DAN PROSEDUR PEMINDAHAN MAKLUMAT

Information Transfer Policies and Procedures

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi:	ICTSO
a) Dasar, prosedur dan kawalan pemindahan maklumat hendaklah diwujudkan;	Pengurus ICT
b) Terma pemindahan maklumat dan perisian di antara jabatan/agensi dengan pembekal hendaklah dimasukkan di dalam perjanjian;	Pentadbir Sistem (Operasi) Pengguna
c) Media yang mengandungi maklumat yang dipindahkan perlu dilindungi; dan	Pembekal
d) Memastikan maklumat yang terdapat dalam emel hendaklah dilindungi.	

9.2.2 PERJANJIAN MENGENAI PEMINDAHAN MAKLUMAT

Agreements on Information Transfer

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Pengurus ICT hendaklah mengawal penghantaran dan penerimaan maklumat organisasi; b) Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat; dan c) Mengenal pasti pihak yang bertanggungjawab ke atas risiko pemindahan maklumat sekiranya berlaku insiden keselamatan maklumat;	ICTSO Pengurus ICT Penyelaras PKP Johor CERT Pentadbir Sistem ICT

9.2.3 PENGURUSAN EMEL

Electronic Messaging

KETERANGAN	TINDAKAN
Mematuhi polisi dan garis panduan penggunaan emel yang berkuat kuasa.	Pentadbir Sistem ICT Personel

9.2.4 PERJANJIAN KERAHSIAAN ATAU MAKLUMAT RAHSIA RASMI

Confidentiality or Non-Disclosure Agreements

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

BIDANG 10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM
Application Acquisition, Development and Maintenance

10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT
Security Requirement of Information System

OBJEKTIF

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

10.1.1 ANALISIS KEPERLUAN DAN SPESIFIKASI KESELAMATAN MAKLUMAT
Information Security Requirement Analysis and Spesification

KETERANGAN	TINDAKAN
Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: a) Semua sistem yang dibangunkan hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan DKICT; b) Merancang penyediaan Pelan Pengurusan Keselamatan Maklumat sistem baharu; c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan;	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

KETERANGAN	TINDAKAN
d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data; dan e) Merancang penilaian tahap keselamatan sistem sebelum sistem baharu diguna pakai.	

10.1.2 KESELAMATAN PERKHIDMATAN SISTEM DI RANGKAIAN AWAM

Securing Application Service on Public Network

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Mengenal pasti dan menentukan tahap kerahsiaan maklumat dan identiti pengguna; b) Mengenal pasti dan menentukan kawalan capaian pengguna; c) Memastikan pengguna dimaklumkan sepenuhnya mengenai kebenaran penggunaan sistem dan perkhidmatan ICT; d) Memastikan pengguna memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen berkaitan; dan e) Mengenal pasti dan menguruskan risiko-risiko yang berkaitan.	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi) Pengguna

10.1.3 MELINDUNGI TRANSAKSI PERKHIDMATAN SISTEM

Protecting Application Service Transaction

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Penggunaan pengesahan identiti secara elektronik oleh setiap pihak yang terlibat dalam transaksi; b) Memastikan kerahsiaan maklumat dan privasi pengguna terjamin; c) Memastikan keselamatan komunikasi dan protokol yang digunakan terjamin; dan d) Mematuhi garis panduan dan peraturan yang berkuat kuasa.	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

Security in Development and Support Process

OBJEKTIF

Memastikan keselamatan maklumat direka bentuk dan dilaksanakan di dalam kitar hayat pembangunan sistem.

10.2.1 DASAR KESELAMATAN PEMBANGUNAN

Secure Development Policy

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

KETERANGAN	TINDAKAN
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.	Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.2 PROSEDUR KAWALAN PERUBAHAN SISTEM

System Change Control Procedure

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengubahsuaian sistem hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Sistem perlu dikaji semula dan diuji apabila terdapat perubahan kepada persekitaran sistem. Pengubahsuaian dan pembetulan yang dilakukan hendaklah dipantau; c) Memastikan perubahan sistem adalah terhad mengikut keperluan yang dibenarkan sahaja; dan d) Akses kepada *source code*, data, perkakasan dan perisian perlu dihadkan kepada pengguna yang dibenarkan sahaja.	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.3 SEMAKAN TEKNIKAL SISTEM SELEPAS PERUBAHAN PLATFORM

Technical Review of Sytem after Operating Platform Change

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; b) Pengujian sistem hendaklah dilakukan apabila berlaku perubahan platform; dan c) Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan perkhidmatan.	ICTSO Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.4 SEKATAN TERHADAP PERUBAHAN PERISIAN DALAM PEMBANGUNAN SISTEM

Restriction on Change to Software Package

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Mengenal pasti risiko sebelum perubahan perisian dilakukan; dan b) Mendapatkan persetujuan daripada pihak yang berkaitan;	ICTSO Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.5 KESELAMATAN PRINSIP KEJURUTERAAN SISTEM

Secure System Engineering Principle

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Prosedur hendaklah diwujudkan, didokumentasi, diselenggara dan diguna pakai dalam pelaksanaan pembangunan sistem berdasarkan prinsip kejuruteraan yang selamat; b) Keselamatan perlu diambil kira dalam semua peringkat pembangunan sistem; dan c) Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa.	Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.6 KESELAMATAN PERSEKITARAN PEMBANGUNAN SISTEM

Secure Development Environment

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Tahap sensitiviti data yang akan diproses, disimpan dan dihantar; b) Mematuhi dasar dan peraturan yang berkuat kuasa; c) Kawalan keselamatan sistem yang dilaksanakan; dan d) Tahap kebolehpercayaan terhadap pengguna berkaitan.	Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

10.2.7 PEMBANGUNAN SISTEM SUMBER LUAR

Outsourced System Development

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Hak harta intelek, *source code* dan data bagi sistem yang dibangunkan adalah menjadi hak milik Kerajaan Negeri Johor; b) Keperluan perjanjian hendaklah merangkumi amalan reka bentuk, pengaturcaraan dan pengujian yang selamat; dan c) Mengenal pasti risiko dan menentukan tahap kawalan keselamatan.	ICTSO Pengurus ICT Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi) Pembekal

10.2.8 PENGUJIAN KESELAMATAN SISTEM

System Security Testing

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Semua sistem baharu dan penambahbaikan sistem hendaklah menjalani ujian dan pengesahan fungsi keselamatan; b) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam sistem bagi menjamin proses dan ketepatan maklumat;	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi)

KETERANGAN	TINDAKAN
c) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam sistem; d) Membuat semakan pengesahan di dalam sistem 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 secara luaran dan dalaman oleh pihak yang bertauliah dalam keselamatan sistem.	

10.2.9 PENGUJIAN PENERIMAAN SISTEM

System Accepting Test

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut: a) Menyediakan persekitaran pengujian yang bersesuaian; b) Memastikan penggunaan data pengujian yang bersesuaian; c) Menyediakan skrip pengujian yang lengkap dan bersesuaian; dan d) Mengenal pasti penguji sistem yang layak dan bersesuaian.	Pemilik Sistem ICT Pembangun Sistem ICT Pentadbir Sistem (Aplikasi) Pengguna

10.3 DATA UJIAN

Test Data

OBJEKTIF

Memastikan data pengujian dilindungi dan dikawal.

10.3.1 PERLINDUNGAN DATA UJIAN

Protection of Test Data

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

BIDANG 11

HUBUNGAN DENGAN PEMBEKAL
Supplier Relationship

11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL
Information Security in Supplier Relationships

OBJEKTIF

Memastikan aset ICT jabatan/agensi yang boleh dicapai oleh pembekal dilindungi.

11.1.1 DASAR KESELAMATAN MAKLUMAT UNTUK HUBUNGAN DENGAN PEMBEKAL
Information Security Policy for Supplier Relationships

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;	ICTSO Pengurus ICT Pembekal

KETERANGAN	TINDAKAN
e) Jenis-jenis obligasi kepada pembekal; f) Pelan kontigensi bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g) Taklimat Keperluan Keselamatan oleh jabatan/agensi kepada pembekal seterusnya menandatangani Surat Akuan Pematuhan DKICT; dan h) Memastikan pembekal melepasi tapisan keselamatan yang ditentukan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).	

11.1.2 MENGENAL PASTI KESELAMATAN DALAM PERJANJIAN PEMBEKAL

Addressing Security within Supplier Agreements

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

11.1.3 RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

Information and Communication Technology Supply Chain

KETERANGAN	TINDAKAN
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat rantaian pembekal bagi menangani risiko. Perkara-perkara yang perlu diambil kira adalah seperti berikut: 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 c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	ICTSO Pengurus ICT Pembekal

11.2 PENGURUSAN PRESTASI PERKHIDMATAN PEMBEKAL

Supplier Service Delivery Management

OBJEKTIF

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan prestasi perkhidmatan adalah sama seperti perjanjian pembekal.

11.2.1 PEMANTAUAN DAN KAJIAN PERKHIDMATAN PEMBEKAL

Monitoring and Review Supplier Services

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; 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.	ICTSO Pengurus ICT Pembekal

11.2.2 PENGURUSAN TERHADAP PERUBAHAN PERKHIDMATAN PEMBEKAL

Managing Changes to Supplier Services

KETERANGAN	TINDAKAN
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;	ICTSO Pengurus ICT Pembekal

KETERANGAN	TINDAKAN
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.	

BIDANG 12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT
Information Security Incident Management

12.1 PENGURUSAN DAN PENAMBAHBAIKAN INSIDEN KESELAMATAN MAKLUMAT
Management of Information Security Incident and Improvement

OBJEKTIF

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

12.1.1 TANGGUNGJAWAB DAN PROSEDUR
Responsibility and Procedure

KETERANGAN	TINDAKAN
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.	ICTSO Pengurus ICT Johor CERT

12.1.2 MEKANISME PELAPORAN INSIDEN

Reporting Information Security Event

KETERANGAN	TINDAKAN
Insiden keselamatan maklumat atau ancaman yang berlaku hendaklah dilaporkan sebagaimana prosedur pelaporan insiden keselamatan maklumat yang berkuat kuasa.	ICTSO Pengurus ICT Johor CERT GCERT

12.1.3 MELAPORKAN KERENTANAN KESELAMATAN MAKLUMAT

Reporting Security Weakness

KETERANGAN	TINDAKAN
Pengguna dan pembekal sistem jabatan/agensi dikehendaki mengambil maklum dan melaporkan kerentanan keselamatan maklumat kepada Pentadbir Sistem ICT.	Pentadbir Sistem ICT Pengguna Pembekal

12.1.4 PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

Assessment of and Decision on Information Security Event

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

12.1.5 RESPON INSIDEN KESELAMATAN MAKLUMAT

Response to Information Security Incident

KETERANGAN	TINDAKAN
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah berkuat kuasa.	ICTSO Johor CERT Agensi Forensik Bertauliah

12.1.6 IKTIBAR DARI INSIDEN KESELAMATAN MAKLUMAT

Learning from Information Security Incidents

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 CERT

12.1.7 PENGUMPULAN BAHAN BUKTI

Collection of Evidence

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

BIDANG 13

ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Information Security Aspects of Services Continuity Management

13.1 KESELAMATAN MAKLUMAT BAGI KESINAMBUNGAN PERKHIDMATAN

Information Security for Service Continuity

OBJEKTIF

Memastikan keselamatan maklumat dalam pengurusan kesinambungan perkhidmatan.

13.1.1 PENGURUSAN KESELAMATAN MAKLUMAT DALAM KESINAMBUNGAN PERKHIDMATAN

Managing Information Security for Service Continuity

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.	CIO ICTSO Pengurus ICT Koordinator PKP Pasukan PKP

13.2 *REDUNDANCY*

Redundancy

OBJEKTIF

Memastikan ketersediaan perkhidmatan melalui mekanisma *redundancy*.

13.2.1 KETERSEDIAAN FASILITI PERKHIDMATAN

Availability of Information Process Facilities

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

BIDANG 14

PEMATUHAN
Compliance

14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN PERJANJIAN KONTRAK
Compliance with Legal and Contractual Requirement

OBJEKTIF

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

14.1.1 MENGENAL PASTI UNDANG-UNDANG DAN PERJANJIAN KONTRAK
Identification of Applicable Legislation and Contractual Agreement

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.	CIO ICTSO Pegawai Undang-undang Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

14.1.2 HAK HARTA INTELEK

Intellectual Property Rights

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.	CIO ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

14.1.3 PERLINDUNGAN REKOD

Protection of Records

KETERANGAN	TINDAKAN
Perkara-perkara yang perlu dipatuhi: a) Keperluan perundangan, peraturan dan perjanjian kontrak; dan b) Melindungi rekod daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan dengan merujuk kepada Arkib Negara dan CGSO.	CIO ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

14.1.4 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

Privacy and Protection of Personally Identifiable Information

KETERANGAN	TINDAKAN
Pengguna hendaklah memberi jaminan dalam melindungi maklumat peribadi seperti tertakluk di dalam keperluan perundangan dan peraturan-peraturan yang berkuat kuasa.	CIO ICTSO Pengurus ICT Pentadbir Sistem ICT Pengguna Pembekal

14.1.5 PERATURAN KAWALAN KRIPTOGRAFI

Regulation of Cryptographic Controls

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

14.2 KAJIAN KESELAMATAN MAKLUMAT

Information Security Reviews

OBJEKTIF

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

14.2.1 KAJIAN BADAN BEBAS TERHADAP KESELAMATAN MAKLUMAT

Independent Review of Information Security

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

14.2.2 PEMATUHAN DASAR DAN STANDARD

Compliance with Security Policy and Standard

KETERANGAN	TINDAKAN
Kerajaan Negeri Johor hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan dasar, standard dan keperluan teknikal yang bersesuaian.	CIO ICTSO

14.2.3 KAJIAN SEMULA PEMATUHAN TEKNIKAL

Technical Compliance Review

KETERANGAN	TINDAKAN
Jabatan/Agensi hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti di dalam dasar, standard dan keperluan teknikal.	CIO Jabatan/Agensi ICTSO Jabatan / Agensi

E. 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 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.
CIO	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
GCERT	Pasukan di bawah MAMPU yang membantu agensi mengendalikan insiden keselamatan ICT.
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.

ISTILAH	KETERANGAN
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.
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.
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.
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 sistem atau 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.
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.
UTILITI *PRIVILEGE*	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.

F. SENARAI PERUNDANGAN DAN PERATURAN - PERATURAN

BIL	SENARAI PERATURAN
1	Arahan Keselamatan.
2	Arahan 20 - Dasar dan Mekanisme Pengurusan Bencana Negara
3	Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara
4	Pekeliling Am Bil.1 Tahun 2015 - Pelaksanaan Data Terbuka Sektor Awam
5	Rancangan Malaysia ke - 11
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
8	Dasar Kriptografi Negara - 12 Julai 2013
9	Surat Pekeliling Perbendaharaan - Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013
10	Pekeliling Perbendaharaan Malaysia PK 2/2013 - Kaedah Perolehan Kerajaan
11	Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia
12	Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013
13	Pegawai Keselamatan Kerajaan 5 Jun 2012 - Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam (Pindaan Kedua)

BIL	SENARAI PERATURAN
14	PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011
15	Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat - 24 November 2010
16	Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam - 22 Januari 2010
17	Akta 709 - Akta Perlindungan Data Peribadi 2010
18	Surat Pekeliling Am Bil.3 Tahun 2009 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam
19	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan - 23 November 2007
20	Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan - 1 Jun 2007
21	Arahan Teknologi Maklumat, MAMPU, 2007
22	Akta 680 - Aktiviti Kerajaan Elektronik 2007
23	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
24	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

BIL	SENARAI PERATURAN
25	Surat Pekeliling Am Bil.4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
26	Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006
27	Akta 658 - Akta Perdagangan Elektronik 2006
28	Surat Pekeliling Am Bil.6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
29	Akta 629 - Akta Arkib Negara 2003
30	Akta 606 - Akta Cakera Optik 2000
31	Akta 588 - Akta Komunikasi dan Multimedia 1998
32	Akta 562 - AktaTandatangan Digital 1997
33	Akta 563 - Akta Jenayah Komputer 1997
34	Akta 564 - Telemedicine Act 1997
35	Akta 88 - Akta Rahsia Rasmi 1972
36	Akta 332 - Akta Hak Cipta 1987
37	Surat Pekeliling Am Bil.2/1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987)
38	Akta 298 - Kawasan Larangan Tempat Larangan 1959 Akta 56 - Akta Keterangan 1950
39	National Cyber Security Policy (NCSP)

BIL	SENARAI PERATURAN
40	Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisations
41	Arahan Tetap Sasaran Penting
42	Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara
43	Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi
44	Perintah Am Bab D
45	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT KERAJAAN NEGERI JOHOR 2.0

NAMA (HURUF BESAR) : _____

NO. KAD PENGENALAN : _____

JAWATAN : _____

BAHAGIAN : _____

Adalah dengan sesungguhnya dan sebenarnya mangaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam DASAR KESELAMATAN ICT KERAJAAN NEGERI JOHOR 2.0 2017; 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 MAKLUMAT NEGERI JOHOR)
TARIKH :

PENGHARGAAN

AHLI JAWATANKUASA PEMURNIAN DASAR KESELAMATAN ICT NEGERI JOHOR

PEJABAT SUKJ BAHAGIAN SAINS TEKNOLOGI DAN ICT	
1	YBM TUNKU ZAHRAH BINTI TUNKU OSMAN *SETIAUSAHA BAHAGIAN* *PEGAWAI KESELAMATAN ICT (ICTSO) JOHOR*
2	ENCIK MD. ROZAMUSLIADI BIN ROSLAN *KETUA PENOLONG SETIAUSAHA BAHAGIAN*
3	ENCIK MOHD. HADDY BIN MD. YATIM *PENOLONG SETIAUSAHA KANAN BAHAGIAN*
4	YM PUAN RAJA EMY ARFAH BINTI RAJA ABD. RAHMAN *PENOLONG SETIAUSAHA BAHAGIAN*
5	ENCIK AZMAN BIN AZMI *PENOLONG SETIAUSAHA BAHAGIAN*
6	ENCIK ONN AZRAAI BIN PUADE *PENOLONG SETIAUSAHA BAHAGIAN*
7	PUAN ZUBAIDAH BINTI ZAIMUDIN *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
8	PUAN NORLELA BINTI YASIN *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
9	ENCIK MOHD. ARIFF BIN MOHD SAMANI *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
10	ENCIK MOHD. HISYAM BIN MUHTAR *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
11	PUAN LYIANA BINTI MUSA *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
12	ENCIK SYED MUHAMMAD BIN SYED HUSSIN *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
13	ENCIK ZAIDI BIN MULIA *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
14	CIK NOR RAHIZATUN BINTI IBRAHIM *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*
15	PUAN NURULHUDA FIRDAUS BINTI MOHDZAR *PENOLONG PEGAWAI TEKNOLOGI MAKLUMAT*

JABATAN / PIHAK BERKUASA TEMPATAN NEGERI JOHOR	
1	PUAN NORZANA BINTI NORDIN *PEGAWAI PENYELIDIK (TEKNOLOGI MAKLUMAT)* *BAHAGIAN PERANCANG EKONOMI NEGERI JOHOR*
2	PUAN WAHIDAH BINTI GAZALI *PEGAWAI TEKNOLOGI MAKLUMAT* *PEJABAT TANAH DAN GALIAN JOHOR*
3	ENCIK MOKHZANI BIN MISLAN *PEGAWAI TEKNOLOGI MAKLUMAT KANAN* *MAJLIS BANDARAYA JOHOR BAHRU*
4	CIK SYARIZA BINTI MOHAMMAD SHARIF *PEGAWAI TEKNOLOGI MAKLUMAT* *MAJLIS PERBANDARAN PASIR GUDANG*
5	PUAN SHAHIDA BINTI AHMAD *PEGAWAI TEKNOLOGI MAKLUMAT* *MAJLIS PERBANDARAN KULAI*
6	PUAN RAFIDAH BINTI RAHMAT *PEGAWAI TEKNOLOGI MAKLUMAT* *MAJLIS PERBANDARAN KLUANG*
7	PUAN HARTINI BINTI SAROH *PEGAWAI TEKNOLOGI MAKLUMAT* *YAYASAN PEMBANGUNAN KELUARGA DARUL TAKZIM*

UNIT PERMODENAN TADBIRAN DAN PERANCANGAN PENGURUSAN MALAYSIA (MAMPU)	
1	PUAN NUR HIDAYAH BINTI ABDULLAH *PERUNDING ICT (PENGURUSAN KESELAMATAN)* *PEGAWAI KESELAMATAN ICT (ICTSO) MAMPU*
2	PUAN ITA NURAZLIN BINTI MOHD SAHLAN *PAKAR ICT (PENGURUSAN KESELAMATAN)*