POLISI KESELAMATAN SIBER

PENTADBIRAN KERAJAAN NEGERI SEMBILAN

VERSI 1.0

POLISI KESELAMATAN SIBER (PKS)

PENTADBIRAN KERAJAAN NEGERI SEMBILAN

VERSI 1.0

KANDUNGAN

SEJARAH DOKUMEN

Kelulusan:
Mesyuarat Jawatankuasa PEMANDU Teknologi Maklumat dan Komunikasi Negeri Sembilan Bil.2/2005

Dasar Keselamatan ICT Negeri Sembilan Darul Khusus Versi 1.0

Tarikh Kuatkuasa:
15 Ogos 2005

Tarikh Kuatkuasa:
3 Sept 2010

Dasar Keselamatan ICT Negeri Sembilan Darul Khusus Versi 2.0

Kelulusan:
Mesyuarat Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS) Bil.3/2010

Kelulusan:
Mesyuarat Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS) Bil.1/2015

Dasar Keselamatan ICT (DKICT) Pentadbiran Kerajaan Negeri Sembilan Versi 2.1

Tarikh Kuatkuasa:
23 Mac 2015

Tarikh Kuatkuasa:
12 Feb 2019

Dasar Keselamatan ICT (DKICT) Pentadbiran Kerajaan Negeri Sembilan Versi 3.0

Kelulusan:
Mesyuarat Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS) Bil.3/2019

REKOD PINDAAN

NAMA DOKUMEN	VERSI	BUTIRAN PINDAAN
Dasar Keselamatan ICT Negeri Sembilan Darul Khusus	1.0	Pindaan Dokumen dengan Merujuk Dasar/ Pekeliling/ Surat Arahan yang Sedang Berkuatkuasa serta Mengambil Kira Keperluan Keselamatan ICT Semasa
Dasar Keselamatan ICT Negeri Sembilan Darul Khusus	2.0	Pindaan Dokumen dengan Merujuk Dasar/ Pekeliling/ Surat Arahan yang Sedang Berkuatkuasa serta Mengambil Kira Keperluan Keselamatan ICT Semasa
Dasar Keselamatan ICT (DKICT) Pentadbiran Kerajaan Negeri Sembilan	2.1	Pindaan Dokumen dengan Merujuk Dasar/ Pekeliling/ Surat Arahan yang Sedang Berkuatkuasa serta Mengambil Kira Keperluan Keselamatan ICT Semasa
Dasar Keselamatan ICT (DKICT) Pentadbiran Kerajaan Negeri Sembilan	3.0	Pindaan Dokumen dengan Merujuk Dasar/ Pekeliling/ Surat Arahan yang Sedang Berkuatkuasa serta Mengambil Kira Keperluan Keselamatan ICT Semasa
Polisi Keselamatan Siber (PKS) Pentadbiran Kerajaan Negeri Sembilan	1.0	• Penjenamaan Semula DKICT kepada Polisi Keselamatan Siber (PKS) merujuk dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) • Tambahan 2 Bidang Baharu i. Bidang 6 – Kriptografi ii. Bidang 11 – Hubungan Pihak Luaran • Tambahan 4 Sub Bidang Baharu i. Sub Bidang 4-3-4 Media Mudah Alih Persendirian (BYOD) ii. Sub Bidang 5-1-3 Pengkomputeran Awan iii. Sub Bidang 7-2-10 Kawalan Peralatan Sewaan/ Ujicuba iv. Sub Bidang 8-8-1 Pengurusan Data Terbuka

SINGKATAN

ISTILAH	KETERANGAN
CDO	*Chief Digital Officer*
CIO	*Chief Information Officer*
CSIRTNS	*Cyber Security Incident Response Team Negeri Sembilan*
DRP	*Disaster Recovery Plan*
ICTSO	*ICT Security Officer*
ISMP	*Information Security Management Plan*
JTICTNS	Jawatankuasa Teknikal ICT Negeri Sembilan
JPICTNS	Jawatankuasa Pemandu ICT Negeri Sembilan
KNS	Kerajaan Negeri Sembilan
NACSA	*National Cyber Security Agency*
PKJ	Pegawai Keselamatan Pejabat
PKP	Pelan Kesinambungan Perkhidmatan
PKS	Polisi Keselamatan Siber

PENGENALAN

Polisi Keselamatan Siber (PKS) Pentadbiran Kerajaan Negeri Sembilan mengandungi peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Polisi ini juga menerangkan kepada semua warga KNS, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di Pentadbiran KNS mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT di ruang siber.

OBJEKTIF

PKS pentadbiran KNS diwujudkan untuk menjamin kesinambungan urusan pentadbiran dan penyampaian perkhidmatan dengan meminimumkan impak insiden keselamatan siber.

Polisi ini bertujuan untuk menyediakan kemudahan perkongsian maklumat yang selamat bagi memenuhi keperluan operasi pentadbiran KNS.

Objektif utama polisi ini adalah seperti berikut:

i. memastikan keselamatan penyampaian perkhidmatan pentadbiran KNS di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi kerajaan, industri dan orang awam.

ii. memastikan kelancaran operasi pentadbiran KNS dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku.

iii. melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang melibatkan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi.

iv. mencegah salah guna atau kecurian Aset ICT Kerajaan.

v. menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan merupakan suatu proses berterusan yang memerlukan aktiviti berkala dari semasa ke semasa untuk menjamin keselamatan.

Keselamatan Siber merujuk kepada kaedah pencegahan yang digunakan untuk melindungi maklumat daripada dicuri, dikompromi, disalah guna atau diserang. Ia memerlukan pemahaman tentang ancaman maklumat yang berpotensi seperti virus, *malware* dan kod jahat yang lain. Strategi keselamatan siber termasuk pengurusan identiti, pengurusan risiko dan pengurusan insiden.

Keselamatan Siber berkait rapat dengan perlindungan Aset ICT yang merangkumi empat asas utama iaitu:

i. melindungi kerahsiaan maklumat rasmi kerajaan.
ii. menjamin setiap maklumat adalah selamat, tepat dan betul.
iii. memastikan ketersediaan maklumat apabila diperlukan oleh warga pentadbiran KNS dan pihak luaran.
iv. memastikan akses dan terimaan maklumat kepada warga pentadbiran KNS dan pihak luaran adalah dari sumber yang sah.

Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

i. kerahsiaan (*confidentiality*) - maklumat tidak boleh didedahkan sewenang-wenangnya atau diakses tanpa kebenaran.
ii. integriti (*integrity*)- data dan maklumat hendaklah tepat, lengkap dan terkini.
iii. ketersediaan (*avaibility*) - data dan maklumat boleh diakses pada bila-bila masa dan di mana-mana jua.

Ketiga-tiga ciri utama keselamatan maklumat ini mestilah dipenuhi bagi menjamin penyampaian perkhidmatan yang berterusan dan selamat kepada warga KNS dan pihak luaran.

SKOP

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

i. data dan maklumat samada digital dan bukan digital hendaklah boleh diakses secara berterusan dengan selamat, tepat, mudah dan dipercayai bagi meningkatkan sistem penyampaian perkhidmatan pentadbiran KNS.
ii. data dan maklumat adalah terjamin kerahsiaannya bagi memastikan kesempurnaan dan kesahihan maklumat serta melindungi kepentingan kerajaan, warga pentadbiran KNS dan pihak luaran.

PKS merangkumi perlindungan semua bentuk maklumat kerajaan samada aktiviti mewujud, menyimpan, menjana, mengakses, mencetak, mengedar dan memusnahkan bagi menentukan keselamatan aset ICT adalah terjamin sepanjang masa. Ini akan dilakukan melalui penguatkuasaan sistem kawalan serta pematuhan prosedur dalam pengendalian semua perkara-perkara berikut:

i. **Perkakasan** *(Hardware)*

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan pentadbiran KNS. Contohnya komputer, pelayan, peralatan mudah alih dan telekomunikasi, peralatan rangkaian dan keselamatan, media storan, IoT dan sebagainya.

ii. **Perisian** *(Software)*

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti:

a. sistem pengoperasian (Windows, Linux/Android, IOS).

b. sistem pangkalan data (MySQL, Oracle, MSSQL).

c. perisian sistem rangkaian dan keselamatan (antivirus, *firewall*, IPS, WAF).

d. sistem Aplikasi (sistem HRMIS, sistem e-Direktori).

iii. **Manusia** *(People)*

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan tugas-tugas dan fungsi yang dilaksanakan bagi mencapai misi dan objektif pentadbiran KNS.

iv. **Data atau Maklumat** *(Data and Information)*

Koleksi fakta-fakta dalam bentuk digital atau bukan digital yang mengandungi maklumat yang digunakan bagi mencapai misi dan objektif pentadbiran KNS. Contohnya dokumentasi, prosedur operasi, rekod, profil pelanggan, pangkalan data, fail data, arkib dan lain-lain.

v. **Perkhidmatan** *(Services: Supporting & Accessibility)*

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

a. perkhidmatan rangkaian seperti LAN, WAN dan lain-lain.

b. sistem kawalan akses seperti sistem kad akses.

c. premis yang digunakan untuk menempatkan aset ICT.

d. perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran, *Uninterruptible Power Supply* (UPS), *Close Circuit Television* (CCTV) dan lain-lain.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada PKS pentadbiran KNS dan perlu dipatuhi adalah seperti berikut:

i. Prinsip "Perlu-Tahu"

Maklumat yang dicapai oleh warga pentadbiran KNS dan pihak luaran hendaklah berdasarkan prinsip "Perlu-Tahu" merujuk kepada peranan dan fungsi kerja masing-masing serta mendapat kebenaran pengurusan.

ii. Hak Akses Minimum

Warga pentadbiran KNS hendaklah diberikan hak akses minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan, tanggungjawab dan bidang tugas.

iii. Akauntabiliti

Prinsip akauntabiliti memerlukan warga pentadbiran KNS bertanggungjawab/ dipertanggungjawabkan ke atas apa sahaja tindakan mereka pada aset ICT. Antara mekanismenya iaitu:

a. menghalang pendedahan maklumat kepada pihak yang tidak berkenaan.

b. memastikan maklumat tepat dan lengkap dari semasa ke semasa dan sedia untuk digunakan.

c. menjaga kerahsiaan kata laluan.

d. mematuhi polisi keselamatan yang ditetapkan.

iv. Pengasingan Tugas

Bagi mengekalkan prinsip semak-dan-imbang *(check and balance)*, warga pentadbiran KNS hendaklah melaksanakan pengasingan tugas kritikal (yang mengendalikan tugas-tugas terperingkat) supaya tidak dilaksanakan oleh seseorang yang bertindak atas kuasa tunggalnya *(single point of failure).*

v. Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada warga pentadbiran KNS yang dibenarkan mengikut peranan dan fungsi tugas yang ditetapkan.

vi. Peminimuman Data

Warga pentadbiran KNS hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang ditetapkan sahaja.

RISIKO

Pentadbiran KNS hendaklah mengenal pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian pentadbiran KNS tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber pentadbiran KNS.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber pentadbiran KNS.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

i. **Kerentanan** *(Vulnerability)*

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

ii. **Ancaman** *(Threat)*

   Pentadbiran KNS hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

iii. **Impak** *(Risk Impact)*

   Pentadbiran KNS hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi pentadbiran KNS.

iv. **Tahap Risiko** *(Risk Level)*

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

v. **Penguraian Risiko** *(Residual Risk)*

   Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/ faedahnya. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

   a) **Teknologi**

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

b) Proses

Perekayasaan proses, prosedur operasi standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

c) Manusia

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

vi. Pengurusan Risiko *(Risk Management)*

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

- mengenal pasti kerentanan.
- mengenal pasti ancaman.
- menilai risiko.
- menentukan penguraian risiko.
- memantau keberkesanan penguraian risiko.
- memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

b) Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** oleh jabatan/ agensi masing-masing dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Negeri Sembilan.

PELAN PENGURUSAN KESELAMATAN MAKLUMAT (PROJEK)

Pelan Pengurusan Keselamatan Maklumat atau *Information Security Management Plan* (ISMP) mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKS Pentadbiran KNS dan surat pekeliling/ arahan terkini.

BIDANG 1

POLISI KESELAMATAN MAKLUMAT

Information Security Policies

BIDANG 1
POLISI KESELAMATAN MAKLUMAT
Information Security Policies

1-1 HALA TUJU PENGURUSAN KESELAMATAN MAKLUMAT
Management Directions for Information Security

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

1-1-1 Polisi Keselamatan Maklumat
Policies for Information Security

Pelaksanaan Polisi Polisi ini dijalankan oleh Setiausaha Kerajaan Negeri Sembilan dengan disokong oleh JPICTNS yang terdiri daripada CDO/ CIO dan ahli-ahli yang dilantik serta disokong oleh prosedur keselamatan semasa yang sedang berkuatkuasa. Polisi ini hendaklah dipatuhi oleh warga KNS dan Pihak Luaran.	Setiausaha Kerajaan Negeri

1-1-2 Kajian Semula Polisi Keselamatan Maklumat
Review of Policies for Information Security

A. Penyebaran Polisi Polisi keselamatan maklumat hendaklah ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan KNS kepada kepada semua warga KNS dan Pihak Luaran.	ICTSO
B. Penyelenggaraan Polisi PKS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar kerajaan dan kepentingan sosial.	JPICTNS dan ICTSO

Kajian semula polisi hendaklah dilaksanakan sekali dalam tempoh **lima tahun atau mengikut keperluan**. Prosedur penyelenggaraan PKS adalah seperti berikut: i. mengenal pasti pindaan dan mengemukakan cadangan secara bertulis kepada Urus Setia PKS. ii. mengemukakan cadangan pindaan yang telah diselaras kepada ICTSO. iii. membentangkan dan mendapatkan perakuan dan kelulusan mesyuarat JPICTNS. iv. memaklumkan PKS versi terkini kepada semua warga KNS dan pihak luaran.	
C. Pengecualian Polisi PKS adalah terpakai kepada semua warga KNS dan Pihak Luaran. Tiada pengecualian diberikan.	Warga KNS dan Pihak Luaran

BIDANG 2

ORGANISASI KESELAMATAN MAKLUMAT

Organization of Information Security

BIDANG 2
ORGANISASI KESELAMATAN MAKLUMAT
Organization of Information Security

2-1 ORGANISASI DALAMAN
Internal Organization

Objektif: Mewujudkan pengurusan organisasi keselamatan untuk melaksana serta mengawal pengoperasian keselamatan maklumat dalam organisasi.

2-1-1 Peranan dan Tanggungjawab Keselamatan Maklumat
Information Security Roles and Responsibilities

A. Setiausaha Kerajaan Negeri Sembilan berperanan dan bertanggungjawab dalam perkara berikut: i. menetapkan hala tuju dan strategi untuk pelaksanaan keselamatan siber bagi semua warga Pentadbiran KNS. ii. memastikan warga KNS memahami dan mematuhi bidang-bidang di dalam PKS. iii. memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan sumber perlindungan keselamatan) adalah mencukupi. iv. memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam PKS. v. merancang, menyelaras dan menyeragamkan pelaksanaan program keselamatan siber Pentadbiran KNS supaya selaras dengan Pelan Strategik Pendigitalan (PSP) SUKNS yang sedang berkuatkuasa. vi. mempengerusikan Mesyuarat JPICTNS.	Setiausaha Kerajaan Negeri

B. Ketua Jabatan/ Agensi berperanan dan bertanggungjawab dalam perkara berikut: i. memastikan pengguna dan pembekal memahami dan mematuhi peruntukan di bawah PKS. ii. memastikan semua keperluan organisasi seperti sumber kewangan, personel dan perlindungan keselamatan maklumat adalah mencukupi. iii. memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam PKS. iv. melantik ICTSO jabatan/ agensi dan Pengurus ICT serta memaklumkan pelantikan kepada warga KNS.	Ketua Jabatan/ Agensi
C. Ketua Pegawai Digital/ Ketua Pegawai Maklumat atau *Chief Digital Officer* (CDO)/ *Chief Information Officer* (CIO) Pentadbiran KNS ialah Timbalan Setiausaha Kerajaan Negeri (Pengurusan), Ketua Jabatan atau pegawai yang dilantik. Peranan dan tanggungjawab CDO/ CIO adalah seperti berikut: i. membantu Setiausaha Kerajaan Negeri Sembilan dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber. ii. menentukan keperluan keselamatan siber. iii. menguatkuasakan PKS. iv. memperkasakan tadbir urus keselamatan siber jabatan/ agensi. v. merancang pelan latihan dan program kesedaran keselamatan siber seperti penyediaan/ pengemaskinian PKS serta pengurusan risiko dan pengauditan. vi. bertanggungjawab ke atas perkara yang berkaitan dengan keselamatan siber Pentadbiran KNS.	CDO/ CIO

D. Pegawai Keselamatan ICT/ ICT *Security Officer* (ICTSO) yang dilantik berperanan dan bertanggungjawab dalam perkara berikut: i. mengurus, menyedia dan melaksanakan keseluruhan program-program keselamatan siber. ii. membantu menguatkuasakan pelaksanaan PKS. iii. memberi penerangan dan pendedahan berkenaan PKS kepada warga KNS. iv. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS. v. menjalankan pengurusan risiko dan keselamatan siber. vi. menjalankan audit, kajian semula, merumus tindak balas pengurusan Pentadbiran KNS berdasarkan hasil penemuan dan menyediakan laporan mengenainya. vii. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. viii. melaporkan insiden keselamatan siber kepada CDO/ CIO dan NACSA sekiranya perlu. ix. bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera. x. menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. xi. bertanggungjawab sebagai Koordinator Pelan Pemulihan Bencana atau *Disaster Recovery Plan* (DRP) jabatan/ agensi.	ICTSO

E. Pengurus ICT merupakan pegawai yang bertanggungjawab menguruskan keselamatan siber meliputi aplikasi, operasi dan rangkaian di bawah kawalannya. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: i. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Pentadbiran KNS. ii. melaksanakan sistem kawalan capaian warga KNS ke atas aset ICT. iii. melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada ICTSO. iv. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber. v. memastikan semua warga Pentadbiran KNS dan pihak luaran yang terlibat dengan jabatan/ agensi mematuhi dasar, piawaian dan garis panduan keselamatan siber dan seterusnya melaporkan sebarang insiden berkaitan. vi. melaksanakan keperluan PKS dalam operasi semasa seperti berikut: a. pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran. b. pembelian atau peningkatan perisian dan sistem computer. c. perolehan teknologi dan perkhidmatan komunikasi. vii. membangunkan garis panduan, prosedur dan tatacara untuk aplikasi khusus (sekiranya perlu). viii. membangun, mengkaji semula dan mengemas kini pelan kontigensi keselamatan siber.	Pengurus ICT

F. Pentadbir Sistem ICT bagi Pentadbiran KNS terdiri daripada: i. Pentadbir Rangkaian dan Keselamatan. ii. Pentadbir Pangkalan Data. iii. Pentadbir Portal/ Laman Web (*Webmaster*). iv. Pentadbir Pusat Data/ Bilik *Server*. v. Pentadbir Sistem Aplikasi. vi. Pentadbir E-mel.	Pentadbir Sistem ICT
G. Pentadbir Rangkaian dan Keselamatan berperanan dan bertanggungjawab seperti berikut: i. memastikan ketersediaan rangkaian setempat (LAN) dan rangkaian luas (WAN) di Pentadbiran KNS. ii. memastikan semua peralatan dan perisian rangkaian dan keselamatan diselenggara. iii. merancang peningkatan infrastruktur, ciri keselamatan dan prestasi rangkaian sedia ada. iv. mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil. v. memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian. vi. memastikan laluan trafik keluar masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian Pentadbiran KNS secara tidak sah. vii. menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian. viii. melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT (SPA) serta penilaian risiko keselamatan maklumat.	Pentadbir Rangkaian dan Keselamatan

H. Pentadbir Pangkalan Data berperanan dan bertanggungjawab seperti berikut: i. melaksanakan polisi pengguna pangkalan data berdasarkan PKS. ii. melaksanakan pemantauan dan penyelenggaraan pangkalan data secara berterusan. iii. memastikan aktiviti pentadbiran pangkalan data seperti kawalan capaian dan proses pengemaskinian data dilaksanakan dengan teratur. iv. melaporkan sebarang insiden berkaitan keselamatan pangkalan data kepada ICTSO.	Pentadbir Pangkalan Data
I. Pentadbir Portal/ Laman Web (*Webmaster*) berperanan dan bertanggungjawab seperti berikut: i. menerima dan memuat naik kandungan portal/ laman web yang telah disahkan oleh pemilik kandungan. ii. memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka. iii. memantau prestasi capaian dan membuat penilaian portal/ laman web secara berkala. iv. memastikan reka bentuk portal/ laman web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi. v. melaksanakan kawalan keselamatan terhadap sistem pengoperasian dan perisian lain di web *server*. vi. melaksanakan proses *backup* dan *restore* secara berkala. vii. melaporkan sebarang isu pelanggaran keselamatan portal/ laman web kepada ICTSO.	Pentadbir Portal/ Laman Web (*Webmaster*)

J. Pentadbir Pusat Data/ Bilik *Server* berperanan dan bertanggungjawab seperti berikut: i. memastikan persekitaran fizikal dan keselamatan Pusat Data/ Bilik *Server* dalam keadaan baik dan selamat. ii. memastikan keselamatan data dan sistem aplikasi di dalam Pusat Data/ Bilik *Server*. iii. melaporkan sebarang pelanggaran keselamatan Pusat Data/ Bilik *Server* kepada ICTSO.	Pentadbir Pusat Data/ Bilik *Server*
K. Pentadbir Sistem Aplikasi berperanan dan bertanggungjawab seperti berikut: i. mengkaji cadangan pembangunan atau penyelenggaraan sistem. ii. membuat kajian semula serta menambah baik sistem sedia ada. iii. membuat pemantauan dan penyelenggaraan terhadap sistem. iv. bertanggungjawab dalam aspek pelaksanaan keseluruhan sistem. v. menyediakan dokumentasi sistem yang berkaitan. vi. memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas. vii. memastikan kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya. viii. mematuhi dan melaksanakan prinsip PKS dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi. ix. melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah seliaannya.	Pentadbir Sistem Aplikasi

L. Pentadbir E-mel berperanan dan bertanggungjawab seperti berikut: i. menentukan setiap akaun yang diwujud atau dibatalkan setelah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar, bersara atau melanggar dasar dan polisi) perlu dilakukan dengan segera atas tujuan keselamatan maklumat. ii. membekukan akaun pengguna semasa pengguna bercuti panjang atau sebab-sebab lain atas arahan Ketua Jabatan. iii. memastikan kemudahan capaian e-mel melalui pelbagai peralatan ICT dan medium komunikasi. iv. melaporkan sebarang pelanggaran penggunaan perkhidmatan e-mel kepada ICTSO.	Pentadbir E-mel
M. Pegawai Aset adalah pegawai yang dilantik oleh Pegawai Pengawal/ Ketua Jabatan/ Pengerusi Jawatankuasa Pengurusan Aset Kerajaan (JKPAK) peringkat jabatan/ agensi yang bertanggungjawab menguruskan aset kerajaan berdasarkan pekeliling yang sedang berkuat kuasa. Pegawai Aset berperanan dan bertanggungjawab: i. terhadap ketersediaan, selenggaraan dan keselamatan aset untuk kegunaan harian. ii. memantau perkakasan ICT yang diagihkan kepada warga KNS.	Pegawai Aset
N. Warga KNS berperanan dan bertanggungjawab seperti berikut: i. membaca, memahami dan mematuhi PKS. ii. mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya. iii. menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat.	Warga KNS

iv. melaksanakan prinsip PKS dan menjaga kerahsiaan maklumat Pentadbiran KNS. v. tidak membuat pendedahan maklumat terperingkat kepada pihak yang tidak berkenaan. vi. memastikan keabsahan maklumat. vii. menjaga kerahsiaan kata laluan. viii. mematuhi piawaian, prosedur dan garis panduan keselamatan siber serta pekeliling/ arahan semasa yang sedang berkuatkuasa. ix. mengaplikasikan pembudayaan keselamatan siber dalam tugasan harian. x. menandatangani Surat Akuan Pematuhan PKS seperti di **Lampiran 1.** xi. mematuhi dan menandatangani Perakuan Akta Rahsia Rasmi 1972 dalam sebarang penyampaian maklumat melalui pelbagai medium komunikasi seperti di **Lampiran 2**. xii. melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera.	
O. Jawatankuasa Pemandu ICT Negeri Sembilan (JPICTNS) merupakan jawatankuasa yang bertanggungjawab dalam keselamatan siber yang berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan siber. Keanggotaan JPICTNS adalah seperti berikut: **Pengerusi:** Setiausaha Kerajaan Negeri **Ahli Tetap:** 1. Pegawai Kewangan Negeri 2. Timbalan Setiausaha Kerajaan Negeri (Pembangunan) 3. Timbalan Setiausaha Kerajaan Negeri (Pengurusan) 4. Pengarah, Unit Pengurusan Teknologi Maklumat	JPICTNS

5. Timbalan Pengarah, Unit Pengurusan Teknologi Maklumat
6. Ketua Jabatan/ Agensi Teknikal:
   - Pejabat Tanah dan Galian Negeri Sembilan
   - Jabatan Kerja Raya Negeri Sembilan
   - PLANMalaysia@Negeri Sembilan
   - Jabatan Pengairan dan Saliran Negeri Sembilan
7. Ketua – Ketua Bahagian/ Unit SUKNS:
   - Unit Pembangunan Ekonomi Negeri (UPEN)
   - Bahagian Kerajaan Tempatan (BKT)
   - Bahagian Perumahan (BP)
   - Bahagian Pembangunan Sumber Manusia (BPSM)
   - Unit Korporat, Inovasi dan Kualiti (UKIK)
8. Pihak Berkuasa Tempatan:
   - Majlis Bandaraya Seremban (MBS)
   - Majlis Perbandaran Port Dickson (MPPD)
9. Ketua Sektor Operasi dan Rangkaian, UPTM
10. Ketua Seksyen Multimedia, Korporat dan Koordinasi ICT, UPTM
11. Ketua Seksyen Pembangunan dan Penyelenggaraan Sistem, UPTM

Urus Setia:

Seksyen Multimedia, Korporat dan Koordinasi ICT (MKK), Unit Pengurusan Teknologi Maklumat (UPTM)

Bidang kuasa JPICTNS adalah seperti berikut:

i. menetapkan arah tuju dan strategi untuk pelaksanaan ICT jabatan/ agensi Pentadbiran Kerajaan Negeri Sembilan.

ii. merancang, mengenalpasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju/ strategi ICT jabatan/ agensi Pentadbiran Kerajaan Negeri Sembilan.

iii. merancang dan menyelaras pelaksanaan program/ projek ICT jabatan/ agensi pentadbiran Kerajaan Negeri supaya selaras dengan Pelan

Strategik Pendigitalan jabatan/ agensi Pentadbiran Kerajaan Negeri Sembilan. iv. menyelaras dan menyeragamkan pelaksanaan ICT antara jabatan/ agensi pentadbiran Kerajaan Negeri dengan Pelan Strategik Pendigitalan Sektor Awam. v. mempromosi dan menggalakkan perkongsian pintar projek-projek ICT antara semua jabatan/ agensi di bawah pentadbiran Kerajaan Negeri. vi. merancang dan menentukan langkah-langkah keselamatan ICT. vii. memantau perkembangan program ICT jabatan/ agensi dan pentadbiran Kerajaan Negeri serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT. viii. menilai dan meluluskan perolehan ICT bagi jabatan/ agensi pentadbiran Kerajaan Negeri berdasarkan had nilai projek. ix. menyelaras dan memantau kemajuan pembangunan dan pelaksanaan projek ICT yang telah diluluskan. x. menyelaras pelaksanaan program-program merapatkan jurang digital peringkat Negeri. **Kekerapan Mesyuarat:** Sekurang-kurangnya empat kali setahun atau mengikut keperluan.	
P. Pasukan Tindak Balas Insiden Keselamatan Siber Negeri Sembilan/ *Cyber Security Incident Response Team* Negeri Sembilan (CSIRTNS) ditubuhkan bagi membantu mengendalikan insiden keselamatan ICT, mengawasi dan memberi nasihat berkaitan keselamatan ICT kepada agensi-agensi di bawah kawalannya. Keanggotaan CERTNS adalah seperti berikut: **Pengerusi:** Pengarah, Unit Pengurusan Teknologi Maklumat (UPTM)	CSIRTNS

Ahli:

1. Timbalan Pengarah, UPTM
2. Ketua Sektor Operasi dan Rangkaian, UPTM
3. Penolong Pengarah, Seksyen Keselamatan, UPTM
4. Penolong Pengarah, Seksyen Rangkaian, UPTM
5. Penolong Pegawai Teknologi Maklumat (Kanan), Seksyen Rangkaian, UPTM
6. Penolong Pegawai Teknologi Maklumat 1, Seksyen Keselamatan, UPTM
7. Penolong Pegawai Teknologi Maklumat 2, Seksyen Keselamatan, UPTM
8. Penolong Pegawai Teknologi Maklumat 1, Seksyen Pembangunan dan Penyelenggaraan Sistem, UPTM
9. Penolong Pegawai Teknologi Maklumat 1, Seksyen Multimedia, Korporat dan Koordinasi ICT, UPTM
10. Juruteknik Komputer 3, Seksyen Operasi, UPTM

Urus Setia:
Seksyen Keselamatan, UPTM

Peranan dan tanggungjawab CSIRTNS adalah seperti berikut:

i. menerima dan mengesan aduan keselamatan siber serta menilai tahap dan jenis insiden.

ii. merekod dan menjalankan siasatan awal insiden yang diterima.

iii. menangani tindak balas insiden keselamatan siber dan mengambil tindakan baik pulih minimum.

iv. menasihati agensi di bawah Pentadbiran KNS supaya mengambil tindakan pemulihan dan pengukuhan.

v. membuat hebahan berkaitan pengukuhan keselamatan siber kepada Pentadbiran KNS. **Kekerapan Mesyuarat:** Sekurang-kurangnya satu kali setahun atau mengikut keperluan.	
Q. Pasukan Kerja Data Terbuka bertanggungjawab dalam menyedia, mengkaji dan mengenalpasti set data yang berpotensi untuk diterbitkan dalam Portal Data Terbuka Sektor Awam. **Pengerusi:** Pengarah, Unit Pengurusan Teknologi Maklumat (UPTM) **Ahli:** 1. Timbalan Pengarah, UPTM 2. Seksyen Multimedia, Korporat dan Koordinasi ICT, UPTM 3. Pentadbir jabatan/ agensi 4. *Editor* jabatan/ agensi **Urus Setia:** Seksyen Multimedia, Korporat & Koordinasi ICT, UPTM **Bidang tugas** Pasukan Kerja Data Terbuka adalah: i. mengkaji dan mengenalpasti set data. ii. mendapatkan kelulusan set data bagi data terbuka. iii. menyedia dan menerbitkan metadata. iv. memastikan set data yang diluluskan bagi data terbuka dimuat naik ke portal/ laman web jabatan/ agensi dan Portal DTSA. v. mengkaji tahap penggunaan data terbuka. **Kekerapan Mesyuarat:** Sekurang-kurangnya satu kali setahun atau ikut keperluan.	Pasukan Kerja Data Terbuka

2-1-2 Pengasingan Tugas *Segregation of Duties*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas Aset ICT. ii. tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi Aset ICT daripada kesilapan, kebocoran maklumat atau dimanipulasi. iii. persekitaran perkakasan yang digunakan bagi tujuan pembangunan sistem aplikasi (*development/ staging*) dan penggunaan sebenar (*production*) hendaklah diasingkan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
2-1-3 Hubungan Pihak Berkuasa *Contact with Authorities*	
Pentadbiran KNS hendaklah memastikan senarai perhubungan dengan pelbagai pihak yang berkaitan diwujud dan dikemas kini. Ia merupakan sumber rujukan warga KNS mengetahui senarai perhubungan pihak berkuasa yang berdekatan. Perkara yang perlu dipatuhi adalah seperti berikut: i. mengenal pasti peraturan yang berkuatkuasa dalam melaksanakan peranan dan tanggungjawab jabatan/ agensi. ii. mewujud dan mengemas kini prosedur/ senarai pihak berkuasa perundangan/ pihak yang dihubungi semasa kecemasan seperti pembekal perkhidmatan, utiliti, kecemasan, keselamatan dan kesihatan. iii. melaporkan sebarang insiden keselamatan dengan segera.	Warga KNS

2-1-4 Hubungan Kumpulan Berkepentingan Yang Khusus *Contact with Special Interest Groups*	
Warga KNS perlu mempunyai hubungan baik dengan pihak berkepentingan yang khusus bagi: i. meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikut perkembangan terkini mengenai keselamatan maklumat. ii. menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini. iii. berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan. iv. berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga KNS
2-1-5 Keselamatan Maklumat dalam Pengurusan Projek ***Information Security in Project Management***	
Pengurusan Projek ICT merupakan satu pengurusan proses dan prosedur dalam satu tempoh masa, sumber dan tahap kualiti yang ditetapkan bagi menghasilkan satu atau lebih produk ICT. Keselamatan maklumat perlu diambil kira dalam pengurusan projek bagi melindungi maklumat dengan merujuk kepada ISMP. Perkara-perkara berikut hendaklah dipatuhi iaitu: i. memastikan objektif keselamatan maklumat dimasukkan di dalam objektif projek. ii. melaksanakan penilaian risiko keselamatan maklumat pada peringkat pelaksanaan projek. iii. memastikan keselamatan maklumat diambil kira semasa pembangunan projek. iv. memastikan implikasi keselamatan maklumat ditangani secara teratur dan berkesan.	Pentadbir Sistem ICT

2-2 PERANTI MUDAH ALIH DAN TELEKERJA
Mobile Devices and Teleworking

Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

2-2-1 Polisi Peranti Mudah Alih
Mobile Device Policy

Peranti mudah alih yang boleh mengumpul, merakam, menyiar dan menyampaikan maklumat dalam apa jua bentuk rekod elektronik perlu diberi kawalan perlindungan bagi memastikan keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. warga KNS bertanggungjawab sepenuhnya terhadap pengurusan dan kawalan keselamatan setiap peranti mudah alih yang dibekalkan. ii. rekod penggunaan peranti mudah alih hendaklah diwujudkan, dikemas kini dan diperiksa. iii. memastikan peranti mudah alih dihindari daripada sebarang ancaman keselamatan maklumat seperti pendedahan, kecurian, pengubahsuaian dan pemalsuan. iv. peranti mudah alih tidak disimpan di dalam kenderaan tanpa pengawasan, di tempat-tempat awam dan premis/ kawasan yang tidak selamat. v. peranti mudah alih yang didapati hilang hendaklah diuruskan berdasarkan kepada pekeliling semasa yang sedang berkuat kuasa.	Warga KNS

2-2-2 Telekerja
Teleworking

Kawalan kemudahan kerja jarak jauh adalah bagi memastikan tiada berlakunya kehilangan peralatan, pendedahan maklumat, capaian tidak sah dan salah guna kemudahan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk melindungi dari risiko	Warga KNS

	penyalahgunaan peranti mudah alih dan kemudahan komunikasi.	
	ii. memastikan bahawa tindakan keselamatan yang bersesuaian diambil untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.	
	iii. memastikan capaian dari luar ke infrastruktur dalaman dengan menggunakan *Virtual Private Network* (VPN).	

BIDANG 3

KESELAMATAN SUMBER MANUSIA

Human Resource Security

BIDANG 3
KESELAMATAN SUMBER MANUSIA
Human Resource Security

3-1 PRA PERKHIDMATAN
Prior To Employment

Objektif: Memastikan semua warga KNS dan pihak luaran memahami tanggungjawab dan peranan masing-masing bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan. Warga KNS dan pihak luaran hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

3-1-1 Tapisan Keselamatan
Security Screening

CDO/ CIO hendaklah memastikan warga KNS dan pihak luaran menjalani tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	CDO/ CIO, Warga KNS dan Pihak Luaran

3-1-2 Terma dan Syarat Perkhidmatan
Terms and Conditions of Employment

Perkara yang perlu dipatuhi adalah seperti berikut: i. warga KNS dan pihak luaran faham dengan jelas peranan dan tanggungjawab masing-masing dalam menjamin keselamatan aset ICT sepanjang tempoh perkhidmatan. ii. warga KNS hendaklah membaca, memahami dan menandatangani Surat Akuan Pematuhan PKS Pentadbiran KNS. iii. warga KNS perlu menjalani tapisan keselamatan sekiranya perlu. iv. pihak luaran perlu menandatangani Surat Akuan Pematuhan PKS, *Non-Disclosure Agreement* (NDA),	ICTSO, Warga KNS dan Pihak Luaran

dan Perakuan Akta Rahsia Rasmi 1972 seperti di **Lampiran 3**. v. warga KNS dan pihak luaran patuh kepada semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	
3-2 DALAM PERKHIDMATAN *During Deployment*	
Objektif: Memastikan warga KNS dan pihak luaran mengetahui tanggungjawab keselamatan maklumat semasa mengendalikan maklumat dan aset ICT.	
3-2-1 Tanggungjawab Pihak Pengurusan *Management Responsibilities*	
Tanggungjawab CDO/ CIO adalah seperti berikut: i. memastikan warga KNS dan pihak luaran mematuhi PKS. ii. memastikan warga KNS dan pihak luaran menguruskan aset ICT berdasarkan perundangan dan peraturan yang berkuatkuasa.	CDO/ CIO
3-2-2 Pembudayaan, Latihan dan Sesi Kesedaran Keselamatan Maklumat *Information Security Awareness, Education and Training*	
Tanggungjawab CDO/ CIO adalah seperti berikut: i. melaksanakan program kesedaran dan pembudayaan yang berkaitan dengan pengurusan keselamatan siber kepada warga KNS dan pihak luaran (sekiranya perlu) secara berterusan. ii. melaksanakan program pemantapan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan siber.	CDO/ CIO

3-2-3 Tindakan Tatatertib *Disciplinary Process*	
Tanggungjawab CDO/ CIO adalah seperti berikut: i. memastikan pemantauan dan penguatkuasaan dilaksanakan secara berterusan. ii. memastikan tindakan perundangan dan tatatertib diambil sekiranya berlaku perlanggaran ke atas sebarang peraturan yang berkuatkuasa berkaitan dengan keselamatan siber.	CDO/ CIO

3-3 PENAMATAN/ PERTUKARAN PERKHIDMATAN
Termination and Change of Employment

Objektif: Melindungi kepentingan dan keselamatan siber secara berterusan disebabkan pertukaran atau penamatan warga KNS serta pihak luaran mengikut peraturan yang ditetapkan dalam terma perkhidmatan.

3-3-1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan *Termination or Change of Employment Responsibilities*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan semua aset ICT dikembalikan. ii. menamatkan kebenaran capaian ke atas maklumat dan kemudahan berkaitan ICT. iii. pihak luaran perlu menandatangani Perakuan Untuk Ditandatangani Komuniti Keselamatan Atau Mana-Mana Pihak Lain Yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat Di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88] seperti di **Lampiran 4**.	ICTSO, Pentadbir Sistem ICT, Pegawai Aset

BIDANG 4

PENGURUSAN ASET

Asset Management

BIDANG 4
PENGURUSAN ASET
Asset Management

4-1 AKAUNTABILITI ASET *Responsibility for Assets*	
Objektif: Memastikan warga KNS bertanggungjawab dalam melindungi semua aset ICT secara komprehensif.	
4-1-1 Inventori Aset ICT *Inventory of Assets*	
Semua Aset ICT diberi kawalan dan perlindungan yang sewajarnya dalam merekod dan mengemas kini maklumat aset mengikut peraturan atau pekeliling semasa yang sedang berkuat kuasa. Setiap aset ICT hendaklah mempunyai maklumat berikut: • pemilik yang sah. • rekod penempatan yang betul.	Pegawai Aset dan Warga KNS
4-1-2 Hak Milik Aset ICT *Ownership of Assets*	
Jabatan/ Agensi perlu memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.	Warga KNS
4-1-3 Penggunaan Aset ICT *Acceptable Use of Assets*	
Perkara berikut perlu dipatuhi dalam penggunaan aset ICT: i. jabatan/ agensi perlu mengenalpasti dan mendokumentasikan aset ICT secara lengkap. ii. warga KNS bertanggungjawab terhadap penggunaan semua aset ICT.	Pegawai Aset dan Warga KNS

iii. pengendalian aset ICT hendaklah merujuk peraturan atau pekeliling semasa yang sedang berkuat kuasa.	
4-1-4 Pemulangan Aset ICT *Return of Assets*	
Warga KNS bertanggungjawab untuk memulangkan aset ICT kepada Pegawai Aset atau pegawai bertanggungjawab apabila bertukar keluar atau meninggalkan perkhidmatan.	Pegawai Aset dan Warga KNS
4-2 PENGELASAN DAN PENGENDALIAN MAKLUMAT *Information Classification*	
Objektif: Memastikan setiap maklumat atau Aset ICT diberikan tahap perlindungan yang bersesuaian.	
4-2-1 Pengelasan Maklumat *Classification of Information*	
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat rahsia rasmi yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan yang sedang berkuat kuasa seperti berikut: i. rahsia besar. ii. rahsia. iii. sulit. iv. terhad. Selain daripada maklumat rahsia rasmi adalah dikelaskan sebagai terbuka.	Warga KNS
4-2-2 Penandaan Maklumat *Labelling of Information*	
Maklumat hendaklah ditanda dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan peraturan prosedur yang ditetapkan Arahan Keselamatan.	Warga KNS

4-2-3 Pengendalian Aset *Handling of Assets*	
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut: i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. ii. memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap. iii. memastikan maklumat sedia untuk digunakan. iv. menjaga kerahsiaan kata laluan. v. mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa. vi. memberi perhatian kepada pengendalian maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.	Pentadbir Sistem ICT dan Warga KNS

4-3 PENGURUSAN MEDIA *Media handling*
Objektif: Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

4-3-1 Pengurusan Media Mudah Alih *Management of Removal Media*	
Media mudah alih merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat. Peraturan yang perlu dipatuhi dalam pengurusan media mudah alih adalah berdasarkan Arahan Keselamatan seperti berikut: i. media mudah alih hendaklah disimpan di tempat penyimpanan yang selamat dan dibenarkan. ii. akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada pentadbir dan pegawai yang dibenarkan sahaja.	Warga KNS

iii. media mudah alih perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan. iv. akses dan pergerakan media mudah alih yang mengandungi data rahsia rasmi hendaklah direkod dan disimpan di tempat penyimpanan yang mempunyai ciri-ciri keselamatan. v. peralatan *backup* bagi media mudah alih hendaklah diletakkan di tempat yang terkawal. vi. mengadakan salinan atau pendua pada media mudah alih bagi tujuan keselamatan dan mengelakkan kehilangan data. vii. hanya maklumat rasmi dibenarkan untuk disimpan dalam media mudah alih yang dibekalkan oleh jabatan/ agensi.	
4-3-2 Pelupusan Media Mudah Alih *Disposal of Media*	
Pelupusan media mudah alih perlu mendapat kelulusan dari Ketua Jabatan/ Agensi dan mengikut prosedur kerajaan yang mana berkenaan. Peraturan yang perlu dipatuhi dalam pelupusan media adalah seperti berikut: i. media mudah alih yang mengandungi maklumat rahsia rasmi yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dengan merujuk peraturan yang berkuat kuasa berkaitan sanitasi media. ii. pelupusan media mudah alih dalam aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa.	Warga KNS
4-3-3 Penghantaran dan Pemindahan *Physical Media Transfer*	
Peraturan yang perlu dipatuhi dalam penghantaran dan pemindahan media adalah berdasarkan Arahan Keselamatan.	Warga KNS

4-3-4 Media Mudah Alih Persendirian *Bring Your Own Device* (BYOD)	
Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut: i. semua maklumat rasmi kerajaan adalah hak milik kerajaan. ii. sebarang bahan rasmi yang dimuat naik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Jabatan. iii. menandatangani Surat Akuan Pematuhan PKS Pentadbiran KNS dan Perakuan Akta Rahsia Rasmi 1972. iv. memastikan media yang digunakan mempunyai kawalan keselamatan seperti berikut: • menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan. • melaksanakan enkripsi dan/ atau perlindungan ke atas fail yang mempunyai maklumat rasmi kerajaan yang disimpan di dalam peranti BYOD. • memastikan BYOD mempunyai ciri-ciri keselamatan seperti antivirus, *patching* terkini dan *anti-theft*. v. warga KNS dilarang daripada melakukan perkara berikut: • menyimpan maklumat rasmi yang sensitif dan rahsia rasmi di dalam BYOD. • menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi yang sensitif dan rahsia rasmi. • menjadikan BYOD sebagai medium sandaran (*backup*) bagi maklumat rasmi. • merakam komunikasi dan dokumen rasmi untuk tujuan peribadi.	Warga KNS

• menjadikan BYOD sebagai *access point* kepada aset ICT jabatan untuk capaian ke internet tanpa kebenaran. vi. warga KNS adalah tertakluk kepada perkara seperti berikut: • menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/ dasar yang berkuat kuasa. • memadam segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ ditamatkan perkhidmatan/ bersara atau sewaktu dihantar untuk penyelenggaraan; • bertanggungjawab dan boleh dikenakan tindakan tatatertib atau tindakan undang-undang sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi kerajaan. • Jabatan/ Agensi berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan atau untuk tujuan siasatan. • Jabatan/ Agensi tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan. • membenarkan pihak Kerajaan untuk membuat analisa risiko ke atas BYOD yang digunakan. • sebarang penggunaaan BYOD adalah tertakluk kepada kelulusan Ketua Jabatan/ Agensi.	

BIDANG 5

KAWALAN CAPAIAN

Access Control

BIDANG 5
KAWALAN CAPAIAN
Access Control

5-1 KEPERLUAN KAWALAN CAPAIAN
Business requirements of access control

Objektif: Mengawal capaian ke atas maklumat/ data dan kemudahan pemprosesan data/ maklumat.

5-1-1 Polisi Kawalan Capaian
Access control policy

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut: i. kawalan capaian ke atas peralatan ICT menepati keperluan keselamatan dan peranan pengguna. ii. kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran. iii. keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih. iv. kawalan ke atas kemudahan pemprosesan maklumat. v. kawalan ke atas capaian sistem aplikasi. vi. kawalan kebenaran untuk menyebarkan maklumat.	CDO/ CIO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

5-1-2 Kawalan Capaian Rangkaian dan Perkhidmatan Rangkaian
Access to Networks and Networks Services

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran daripada Pengurus ICT. Kawalan capaian	ICTSO,

perkhidmatan rangkaian hendaklah dijamin selamat dengan: i. memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian. ii. menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian pentadbiran KNS, rangkaian jabatan/ agensi lain dan rangkaian awam. iii. mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar.	Pengurus ICT, Pentadbir Sistem ICT dan Warga KNS
5-1-3 Pengkomputeran Awan *Cloud Computing*	
Perkara yang perlu dipatuhi bagi perkhidmatan pengkomputeran awan di jabatan/ agensi adalah seperti berikut: i. penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan Ketua Jabatan/ Agensi. ii. pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat. iii. penggunaan pengkomputeran awan (*cloud computing*) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh Ketua Jabatan/ Agensi serta tertakluk kepada arahan-arahan yang dikeluarkan oleh kerajaan dari semasa ke semasa. iv. pelaksanaan pengkomputeran awan yang menyeluruh hendaklah merujuk kepada Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam yang sedang berkuatkuasa.	Ketua Jabatan/ Agensi, ICTSO, Pengurus ICT, Pentadbir Sistem ICT

5-2 PENGURUSAN CAPAIAN PENGGUNA
User Access Management

Objektif: Memastikan kawalan capaian warga KNS yang diperakukan sahaja dan menghalang capaian yang tidak dibenarkan kepada perkhidmatan ICT.

5-2-1 Pendaftaran dan Pembatalan Akaun Pengguna
User Registration and De-Registration

Mewujudkan prosedur pendaftaran dan pembatalan akaun pengguna bagi mengurus capaian dan pembatalan hak capaian. Perkara yang perlu dipatuhi adalah seperti berikut: i. pendaftaran dan penamatan akaun pengguna hendaklah menggunakan borang yang dibenarkan sahaja. ii. akaun pengguna yang diperuntukkan oleh Pengurus ICT hendaklah digunakan untuk tujuan rasmi. iii. akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna. iv. akaun pengguna luar yang diwujudkan diberi tahap capaian dan tempoh masa mengikut peranan dan tanggungjawab pengguna dengan kelulusan Pengurus ICT. v. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ianya tertakluk kepada peraturan dan arahan semasa. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan yang telah ditetapkan. vi. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali atas sebab-sebab tertentu. vii. Pentadbir Sistem ICT boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut: a. pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan/ Agensi.	ICTSO, Ketua Jabatan/ Agensi, Pengurus ICT dan Pentadbir Sistem ICT

b. pengguna yang bercuti melebihi tempoh enam bulan atau seperti mana yang diluluskan oleh Ketua Jabatan/ Agensi. c. bertukar bidang tugas kerja. d. bertukar/ bersara/ meninggal dunia. viii. Pentadbir Sistem ICT boleh membuat tindakan pembatalan serta-merta terhadap pengguna berikut: - a. ditamatkan perkhidmatan: pembatalan serta merta. b. dalam prosiding dan/ atau dikenakan tindakan tatatertib bagi tujuan dibuang kerja: pembatalan serta merta. ix. akaun pengguna yang terlibat dalam proses penyiasatan insiden keselamatan akan dibekukan sementara.	
5-2-2 Penyediaan dan Semakan Capaian Pengguna *User Access Provisioning*	
Mewujudkan prosedur penyediaan capaian pengguna atau pembatalan capaian pengguna kepada perkhidmatan ICT. Perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan hak capaian pengguna hanya kepada yang dibenarkan sahaja atau mengikut bidang tugas. ii. mengemas kini hak capaian pengguna secara berkala atau mengikut keperluan. iii. membatalkan hak capaian pengguna sekiranya bertukar bidang tugas, bertukar keluar, tamat perkhidmatan, dibuang kerja atau bersara.	Pentadbir Sistem ICT
5-2-3 Pengurusan Hak Capaian Khas Pengguna *Management of Privileged Access Rights*	
Peruntukan dan penggunaan *Priviledge Access Rights* perlu dihad dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan bidang tugas. Hak capaian khas pengguna adalah seperti *Administrators Priviledge* dan *Super User Priviledge.*	Pentadbir Sistem ICT

5-2-4 Pengurusan Kata Laluan Pengguna *Management of Secret Authentication Information of Users*	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang telah ditetapkan seperti berikut: i. kata laluan hendaklah dilindungi dan tidak boleh dikongsi. ii. pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau telah dikompromi. iii. panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara besar dan kecil, nombor dan aksara khusus kecuali bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan terhad. iv. kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan. Penggunaan aplikasi *password manager* adalah digalakkan. v. kata laluan log masuk komputer dan *screen saver* hendaklah diaktifkan. vi. kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan. vii. kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas kata laluan diset semula. viii. kata laluan hendaklah berlainan dengan pengenalan identiti pengguna. ix. kata laluan hendaklah ditukar sekurang-kurangnya sekali dalam tempoh enam bulan. x. mengelakkan penggunaan semula kata laluan yang terdahulu. xi. penggunaan *Multi-Factor Authentication* (MFA) adalah digalakkan. xii. kata laluan pengguna hendaklah melalui proses enkripsi apabila disimpan di dalam pangkalan data.	Pentadbir Sistem ICT dan Warga KNS

5-2-5 Semakan Hak Capaian Pengguna *Review of User Access Right*	
Mengkaji semula hak capaian pengguna secara berkala **sekurang - kurangnya satu kali setahun atau mengikut keperluan**.	Pentadbir Sistem ICT
5-2-6 Pembatalan atau Pelarasan Hak Capaian Pengguna *Removal or Adjustment of Access Rights*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. hak capaian pengguna untuk kemudahan pemprosesan data dan maklumat hendaklah dibatalkan selepas penamatan perkhidmatan, kontrak atau perjanjian. ii. pelarasan hak capaian pengguna perlulah dilakukan apabila berlaku perubahan dalaman atau perubahan bidang tugas. iii. hak capaian pengguna hendaklah dibatalkan sekiranya berlaku salah laku kemudahan hak capaian.	Pentadbir Sistem ICT
5-3 TANGGUNGJAWAB PENGGUNA *User responsibilities*	
Objektif: Memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan untuk pengesahan identiti.	
5-3-1 Pematuhan Kata Laluan Pengguna *User Password Compliance*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. mematuhi amalan terbaik pemilihan dan penggunaan kata laluan yang selamat. ii. memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya. iii. mematuhi amalan polisi *clear desk & clear screen*.	Warga KNS

5-3-2 Kawalan Penggunaan Program atau Perisian Khas Utiliti *Use of Privileged Utility Programs*	
Penggunaan program utiliti perlu dikawal dan mematuhi perkara berikut: i. hanya program atau perisian khas utiliti yang selamat sahaja digunakan. ii. penggunaan program atau perisian khas utiliti yang membebankan kapasiti rangkaian (*bandwidth*) perlu dihadkan dan dikawal.	ICTSO
5-3-3 Kawalan Capaian Kod Sumber Program ***Access Control to Program Source Code***	
Perkara yang perlu dipatuhi adalah seperti berikut: i. pembangunan kod sumber program perlu diselia, dipantau dan boleh dicapai oleh pemilik sistem. ii. kod sumber bagi semua sistem/ aplikasi adalah menjadi hak milik kerajaan. iii. kod sumber sesuatu perkhidmatan digital hendaklah disimpan dengan teratur dan selamat. iv. sebarang pindaan kod sumber mestilah mengikut prosedur yang ditetapkan. v. log audit perlu dikekalkan kepada semua capaian kepada kod sumber.	Pentadbir Sistem Aplikasi dan Pengurus ICT

BIDANG 6

KRIPTOGRAFI

Cryptography

BIDANG 6
KRIPTOGRAFI
Cryptography

6-1 KAWALAN KRIPTOGRAFI *Cryptographic Controls*	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat.	
6-1-1 Polisi Kawalan Penggunaan Kriptografi *Policy on the Use of Cryptographic Controls*	
Jabatan/ Agensi perlu memastikan penggunaan kriptografi dilaksanakan dengan mematuhi perkara seperti berikut: i. melaksanakan peraturan enkripsi untuk melindungi maklumat rahsia rasmi atau sensitif menggunakan kaedah kriptografi yang sesuai. ii. mengenal pasti tahap perlindungan penggunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan. iii. warga KNS hendaklah menggunakan kriptografi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	CDO/ CIO, ICTSO Pentadbir Sistem ICT dan Warga KNS
6-1-2 Pengurusan Kunci Kriptografi *Key Management*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. pengurusan ke atas kunci kriptografi hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	CDO/ CIO, ICTSO, Pentadbir Sistem ICT dan Warga KNS

ii. memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di Pentadbiran KNS. iii. setiap urusan transaksi maklumat sensitif hendaklah menggunakan tandatangan digital atau kunci kriptografi supaya mendapat perlindungan dan pengiktirafan undang - undang. Penggunaan tandatangan digital hendaklah dilaksanakan bagi pengurusan transaksi maklumat rahsia rasmi secara elektronik.	

BIDANG 7

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Physical and Environmental Security

BIDANG 7
KESELAMATAN FIZIKAL DAN PERSEKITARAN
Physical and Environmental Security

7-1 KESELAMATAN KAWASAN
Secure Areas

Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta capaian yang tidak dibenarkan.

7-1-1 Kawalan Keselamatan Fizikal
Physical Security Perimeter

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara yang perlu dipatuhi adalah seperti berikut: i. kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung pada keperluan untuk melindungi aset. ii. menggunakan kawalan keselamatan parameter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat. iii. memasang alat penggera atau kamera litar tertutup (CCTV). iv. menghadkan jalan keluar masuk. v. mengadakan kaunter kawalan. vi. menyediakan ruang atau bilik khas untuk pelawat. vii. mewujudkan perkhidmatan kawalan keselamatan. viii. melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini.	Pegawai Keselamatan Jabatan dan Pentadbir Sistem ICT

ix. mereka bentuk dan melaksanakan keselamatan perlindungan fizikal di dalam pejabat, bilik serta kemudahan daripada kebakaran, banjir, letupan, kacau bilau dan bencana. x. memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
7-1-2 Kawalan Masuk Fizikal *Physical Entry Controls*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. setiap pegawai dan kakitangan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas. ii. semua pas keselamatan hendaklah diserahkan balik kepada Pegawai Keselamatan atau pihak pengurusan apabila warga KNS berhenti atau bersara. iii. setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama premis kerajaan. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. iv. kehilangan pas mestilah dilaporkan dengan segera.	Warga KNS dan Pihak Luaran
7-1-3 Kawalan Keselamatan Pejabat, Bilik dan Kemudahan ICT *Securing Offices, Rooms and Facilities ICT*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. kawasan tempat bekerja, bilik dan kemudahan ICT perlu dihadkan daripada akses oleh pengguna yang tidak berkaitan. ii. penunjuk ke lokasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	CDO/ CIO, ICTSO, Pengurus ICT, Pegawai Keselamatan Jabatan dan Pentadbir Sistem ICT
7-1-4 Kawalan Perlindungan Ancaman Luar dan Bencana Alam *Protecting Against External and Environmental Threats*	
Perkara yang perlu dipatuhi adalah seperti berikut:	

i. mereka bentuk, melaksana dan membuat kajian semula pelan perlindungan fizikal daripada kebakaran, banjir dan bencana alam. ii. memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau bilau, rusuhan dan sebagainya.	Pegawai Keselamatan Jabatan
7-1-5 Kawalan Tempat Larangan *Working in Secure Areas*	
Kawasan larangan mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas premis tersebut adalah seperti berikut: i. akses kepada kawasan larangan hanya kepada pegawai- pegawai yang dibenarkan sahaja. ii. pihak luaran adalah dilarang untuk memasuki kawasan larangan kecuali dengan kebenaran untuk kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mereka hendaklah dipantau sehingga tugas di kawasan berkenaan selesai. iii. kawasan tempat larangan perlu dikunci pada setiap masa. iv. sebarang bentuk rakaman seperti fotografi, video, audio adalah tidak dibenarkan. v. warga KNS yang perlu berurusan di pusat data / bilik *server* hendaklah mendapatkan kebenaran dan mengisi buku log keluar masuk. Rujuk Garis Panduan Pengurusan Pusat Data MAMPU atau garis panduan jabatan/ agensi yang berkuatkuasa.	Pegawai Keselamatan Jabatan
7-1-6 Kawasan Penghantaran dan Pemunggahan *Delivery and Loading Areas*	
Memastikan kawasan penghantaran dan pemunggahan serta tempat berkaitan dikawal daripada pihak yang tidak diberi kebenaran.	Pegawai Keselamatan Jabatan

7-2 KESELAMATAN PERALATAN ICT
Security of ICT Equipment

Objektif: Melindungi peralatan ICT yang mempunyai fungsi ICT jabatan daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan yang menyebabkan perkhidmatan fasiliti terjejas.

7-2-1 Penempatan dan Perlindungan Peralatan ICT
Placement and Protection of ICT Equipment

Perkara yang perlu dipatuhi adalah seperti berikut: i. warga KNS hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. ii. warga KNS bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang ditetapkan. iii. warga KNS dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan. iv. warga KNS dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT. v. warga KNS adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya. vi. warga KNS perlu memastikan perisian antivirus sentiasa aktif (*activated*), dikemas kini dan melakukan imbasan ke atas media storan yang digunakan. vii. penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. Kerahsiaan kata laluan adalah di bawah tanggungjawab pengguna dan dilarang berkongsi. viii. semua aset sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. ix. peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS).	Pengurus ICT, Pentadbir Sistem ICT dan Warga KNS

x. semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan dalam rak khas dan berkunci. xi. semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai. xii. peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO/ Pengurus ICT dan Pegawai Aset dengan segera. xiii. pengendalian aset ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa. xiv. warga KNS tidak dibenarkan mengubah kedudukan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pengurus ICT / Pentadbir Sistem ICT. xv. sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk baik pulih. xvi. sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin aset tersebut sentiasa berkeadaan baik. xvii. konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal. xviii. warga KNS dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT. xix. warga KNS bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya serta hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja. xx. warga KNS hendaklah memastikan semua perkakasan ICT dalam keadaan dimatikan (*off*) apabila meninggalkan pejabat.	

xxi. memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti kilat, litar pintas dan sebagainya.	
7-2-2 Peralatan Sokongan ICT *Supporting Utilities*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran. ii. peralatan sokongan seperti UPS atau penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di pusat data/ bilik *server* supaya mendapat bekalan kuasa berterusan. iii. semua peralatan sokongan ICT perlu disemak dan di selenggara dari masa ke semasa (sekurang-kurangnya setahun sekali).	ICTSO, Pengurus ICT dan Pentadbir Pusat Data/ Bilik *Server*
7-2-3 Kawalan Keselamatan Kabel *Cabling Security*	
Kabel termasuk kabel elektrik peralatan ICT atau telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah keselamatan yang perlu diambil adalah seperti berikut: i. memastikan hanya Pengurus ICT atau pihak luaran yang dibenarkan boleh melaksanakan pemasangan atau penyelenggaraan kabel. ii. menggunakan kabel mengikut spesifikasi yang telah ditetapkan. iii. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. iv. melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*. v. semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan	ICTSO, Pentadbir Rangkaian, Pentadbir Pusat Data/ Bilik *Server* dan Pihak Luaran

keselamatan kabel daripada kerosakan dan pintasan maklumat.	
7-2-4 Penyelenggaraan Peralatan ICT ***Equipment Maintenance***	
Peralatan ICT hendaklah diselenggara bagi memastikan kebolehsediaan, kerahsiaan dan integriti data/ maklumat terjamin dengan mengambil langkah-langkah seperti berikut: i. semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar. ii. memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja. iii. Pentadbir Sistem ICT bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah tamat tempoh jaminan. iv. menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan serta memastikan laporan penyelenggaraan disediakan. v. memaklumkan warga KNS sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau mengikut keperluan.	Pentadbir Sistem ICT dan Pegawai Aset
7-2-5 Pergerakkan dan Peminjaman Peralatan ICT ***Removal of Assets***	
Perkara yang perlu dipatuhi adalah seperti berikut: i. peralatan ICT yang hendak dibawa keluar dari penempatan yang didaftarkan perlulah mendapat kelulusan dan direkod serta diperakukan pegawai yang dilantik. ii. peralatan ICT yang hendak dialihkan kedudukan hendaklah dimaklumkan kepada Pegawai Aset. iii. peralatan ICT yang dibawa keluar dari premis hendaklah bagi tujuan rasmi sahaja dan perlu mendapatkan kelulusan.	Pegawai Aset dan Warga KNS

iv. aktiviti peminjaman dan pemulangan peralatan ICT mestilah direkodkan oleh pegawai yang dilantik.	
7-2-6 Keselamatan Peralatan ICT Luar Premis *Security of Equipment and Assets Off-Premises*	
Peralatan yang dibawa keluar dari premis adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan peralatan ICT tersebut direkod oleh pegawai yang dilantik. ii. peralatan ICT tersebut perlu dilindungi dan dikawal sepanjang masa. iii. penyimpanan atau penempatan peralatan ICT tersebut mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. iv. menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap. v. sebarang kehilangan peralatan adalah di bawah tanggungjawab pengguna yang membawa keluar peralatan tersebut.	Warga KNS
7-2-7 Keselamatan Semasa Pelupusan dan Penggunaan Semula *Secure Disposal or Reuse of Equipment*	
Pelupusan atau penggunaan semula peralatan ICT melibatkan peralatan yang usang, rosak dan tidak boleh dibaiki. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa dan perkara yang perlu dipatuhi adalah seperti berikut: i. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan (sanitasi data/ media) terlebih dahulu sebelum pelupusan dilaksanakan. ii. Sekiranya maklumat perlu disimpan, warga KNS perlu membuat salinan pendua *(backup).* iii. data-data dalam storan peralatan ICT yang akan dilupuskan secara pindah milik hendaklah dihapuskan dengan cara yang selamat.	Pegawai Aset dan Warga KNS

iv. peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut. v. pegawai yang dilantik hendaklah merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT dalam kad harta modal mengikut tatacara pengurusan aset atau sistem yang sedang berkuat kuasa. vi. pelupusan peralatan ICT hendaklah mengikut tatacara pelupusan semasa yang berkuat kuasa. vii. warga KNS adalah dilarang daripada melakukan perkara seperti berikut: a) menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. b) mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *Control Processing Unit* (CPU) seperti *RAM, hard disk, motherboard* dan sebagainya. c) menyimpan dan memindahkan perkakasan luaran komputer seperti Automatic Voltage Regulator (AVR), *speaker* dan mana-mana peralatan yang berkaitan. d) melupuskan sendiri peralatan ICT. e) memindah keluar dari premis mana-mana peralatan ICT yang hendak dilupuskan. f) memastikan segala maklumat sulit dan rahsia di dalam peralatan disalin pada media storan kedua sebelum menghapuskan maklumat secara kekal.	
7-2-8 Peralatan ICT Gunasama *Unattended User Equipment*	
Warga KNS perlu memastikan bahawa peralatan ICT guna sama dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:	Warga KNS

i. menggunakan ID pengguna dan kata laluan yang diberikan. ii. memastikan peralatan ICT tersebut digunakan oleh pengguna yang dibenarkan sahaja.	
7-2-9 Polisi *Clear Desk* dan *Clear Screen* *Clear Desk and Clear Screen Policy*	
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila pengguna tidak berada di tempatnya. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. menggunakan kemudahan *password screen saver, logout* apabila meninggalkan komputer atau perisian yang bersesuaian. ii. menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci. iii. memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat. iv. memastikan media storan mudah alih tidak ditinggalkan di komputer atau di ruang kerja.	Warga KNS
7-2-10 Kawalan Peralatan Sewaan/ Ujicuba *Proof of Concept*	
Perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir Sistem ICT dan Warga KNS

i. Penerimaan Peralatan yang diterima bebas daripada virus, *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT. **ii. Penyelenggaraan** a) capaian melalui rangkaian luar adalah tidak dibenarkan namun tertakluk kepada kebenaran Pentadbir Sistem ICT. b) aktiviti penyelenggaraan adalah di bawah pengawasan Pentadbir Sistem ICT. **iii. Pemulangan** a) maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*). b) memastikan semua maklumat organisasi tidak tertinggal pada peralatan.	

BIDANG 8

KESELAMATAN OPERASI

Operations Security

BIDANG 8
KESELAMATAN OPERASI
Operations Security

8-1 TANGGUNGJAWAB DAN PROSEDUR OPERASI
Operational Procedures and Responsibilities

Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

8-1-1 Dokumen Prosedur Operasi
Documented Operating Procedures

Perkara yang perlu dipatuhi adalah seperti berikut: i. semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal. ii. setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur, lengkap dan hendaklah dikemas kini mengikut keperluan.	Pentadbir Sistem ICT dan Warga KNS

8-1-2 Kawalan Perubahan
Change Management

Perkara yang perlu dipatuhi adalah seperti berikut: i. peningkatan atau pengubahsuaian yang melibatkan perkakasan, perisian, sistem rangkaian, sistem aplikasi, dan prosedur hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT/ Pemilik Sistem atau pemilik aset ICT dan direkodkan. ii. semua aktiviti seperti memasang, menyelenggara dan mengemaskini mana-mana komponen aset ICT hendaklah dikendalikan oleh pegawai atau pihak yang diberi kebenaran.	Pentadbir Sistem ICT dan Warga KNS

iii. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah dipersetujui serta mematuhi spesifikasi perubahan yang telah ditetapkan. iv. semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan, diperakui, disimpan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
8-1-3 Perancangan Kapasiti *Capacity Management*	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal bagi memenuhi perancangan keperluan semasa dan akan datang. Ia perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT
8-1-4 Pengasingan Persekitaran Pembangunan, Pengujian, Latihan dan Operasi *Separation of Development, Testing, Training and Operation*	
Mewujudkan persekitaran yang berasingan bagi pembangunan sistem aplikasi, pengujian, latihan dan operasi bertujuan mengurangkan risiko capaian tidak sah atau perubahan yang tidak dibenarkan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
8-2 PERLINDUNGAN *MALWARE* ATAU VIRUS *Protection from Malware/ Virus*	
Objektif: Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan disebabkan oleh perisian berbahaya seperti *malware,* virus dan sebagainya.	
8-2-1 Perlindungan daripada Perisian Berbahaya *Controls Against Malware*	
Perkara yang perlu dipatuhi adalah seperti berikut: i. memasang kawalan keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Content Filtering* dan *Web Application*	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

Firewall (WAF) serta mengikut prosedur penggunaan yang betul dan selamat. ii. penggunaan perisian tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa. iii. mengimbas semua perisian dan sistem dengan antivirus sebelum instalasi atau penggunaannya. iv. mengemas kini antivirus dengan *signature* antivirus yang terkini. v. mengemaskini *patches* sistem operasi mengikut keperluan. vi. menyemak fail sistem dan pangkalan data bagi mengesan aktiviti yang tidak diingini seperti kehilangan atau kerosakan maklumat. vii. mengadakan program atau prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. viii. memaklumkan pengguna mengenai ancaman keselamatan ICT seperti serangan *malware*, virus dan sebagainya.	
8-3 SALINAN PENDUA *Backup*	
Objektif: Memastikan sistem, aplikasi, data, imej dan maklumat mempunyai salinan pendua, berkeupayaan untuk *restore* semula bagi melindungi daripada kehilangan maklumat.	
8-3-1 Maklumat Pendua *Information Backup*	
Pelaksanaan *backup* hendaklah dibuat ke atas sistem aplikasi bagi melindungi data atau maklumat daripada hilang. Perkara yang perlu dipatuhi adalah seperti berikut: i. melaksanakan *backup* kepada semua sistem aplikasi kritikal secara harian, mingguan dan bulanan. ii. menguji operasi *backup* dan *restore* sekurang-kurangnya sekali setahun.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

iii. memastikan sistem *backup* berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. iv. merekod dan menyimpan salinan *backup* di lokasi yang berlainan (off-site) dan selamat.	
8-4 LOG DAN PEMANTAUAN *Logging and Monitoring*	
Objektif: Memastikan log direkodkan dan menjana pembuktian melalui pemantauan.	
8-4-1 Log Aktiviti *Event Logging*	
Memastikan setiap peralatan ICT menyimpan log bagi merekod aktiviti pengguna, *exceptions, faults* dan log keselamatan maklumat. Log ini hendaklah dijana, disimpan dan disemak secara berkala. Perkara yang perlu dipatuhi adalah seperti berikut: i. merekod setiap aktiviti transaksi secara berpusat atau tertakluk kepada keperluan. ii. mengandungi ID pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan. iii. memastikan aktiviti capaian pengguna ke atas sistem ICT adalah sah. iv. mengenal pasti aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. v. menyimpan log audit untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian. vi. memastikan masa (*time stamp*) dalam sistem yang diselaraskan dengan suatu masa yang dipersetujui. vii. memastikan analisa ke atas log dilaksanakan secara berkala atau mengikut keperluan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

8-4-2 Kawalan Perlindungan Log *Protection of Log*	
Perkara yang mesti dipatuhi adalah seperti berikut: i. melindungi maklumat log daripada capaian yang tidak dibenarkan. ii. capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja. iii. memastikan log fail tidak boleh diubah. iv. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. v. Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
8-4-3 Log Pentadbir dan Pengendali (Operator) *Administrator and Operator Log*	
Perkara yang mesti dipatuhi adalah seperti berikut: i. memastikan setiap aktiviti log bagi pentadbir dan pengguna sistem direkodkan. ii. melindungi aktiviti log pentadbir dan pengguna sistem daripada capaian yang tidak sah atau hanya yang dibenarkan sahaja. iii. memastikan log sentiasa dipantau dan disemak secara berkala atau mengikut keperluan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
8-4-4 Penyeragaman Waktu *Clock Synchronisation*	
Waktu bagi sistem, perkhidmatan digital atau peralatan ICT hendaklah diselaraskan dengan waktu standard Malaysia.	Pengurus ICT dan Pentadbir Sistem ICT

8-5 KAWALAN PERISIAN OPERASI *Control of Operational Software*	
Objektif: Melindungi sistem operasi dan memastikan integriti sistem operasi.	
8-5-1 Instalasi Perisian Pada Sistem Operasi *Installation of Software Systems*	
Memastikan pelaksanaan kawalan ke atas instalasi perisian pada sistem operasi. Perkara yang mesti dipatuhi adalah seperti berikut: i. pengemaskinian perisian operasi, sistem aplikasi dan program *libraries* hanya boleh dilakukan oleh Pentadbir Sistem ICT dengan mendapat kelulusan Pengurus ICT. ii. instalasi perisian hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT. iii. memastikan penggunaan perisian yang tulen dan mempunyai lesen sah.	Pengurus ICT, Pentadbir Sistem ICT dan Warga KNS
8-6 PENGURUSAN KERENTANAN *Operational Vulnerability Management*	
Objektif: Melindungi dan mencegah daripada berlaku insiden keselamatan siber.	
8-6-1 Pengurusan Ancaman Siber *Management of Technical Vulnerabilities*	
Perkara yang mesti dipatuhi adalah seperti berikut: i. melaksanakan ujian penembusan keselamatan. ii. mengambil tindakan pengukuhan yang bersesuaian bagi meminimakan risiko yang telah dikenalpasti. iii. menyedia dan membuat edaran laporan tindakan pengukuhan yang telah diambil.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
8-6-2 Kawalan Pemasangan Perisian *Restrictions on Software Installation*	
Perkara yang mesti dipatuhi adalah seperti berikut: i. memasang dan menggunakan hanya perisian yang tulen dan mempunyai lesen yang sah.	Warga KNS

ii. mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	

8-7 MEDIA SOSIAL
Social Media

Objektif: Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.

8-7-1 Keselamatan Media Sosial
Security of Social Media

Keselamatan media sosial merupakan kawalan yang digunakan dalam mengelakkan ancaman keselamatan melalui pemantauan keselamatan siber. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara. ii. tidak melibatkan penyebaran maklumat dan dokumen terperingkat. iii. tidak memaparkan kenyataan yang boleh menjejaskan imej kerajaan. iv. tidak menyentuh isu sensitif seperti agama, politik dan perkauman. v. tidak memaparkan kenyataan yang berunsur fitnah atau hasutan. vi. tidak menyebarkan berita yang tidak sahih. vii. tidak melibatkan diri dengan aktiviti yang boleh menjurus kepada *CyberStalking* atau *CyberHarassment*. viii. tidak menggunakan media sosial untuk tujuan peribadi semasa waktu pejabat sama ada menerusi komputer/ peranti mudah alih yang dibekalkan oleh kerajaan. ix. mematuhi dasar dan peraturan semasa berkaitan media sosial yang sedang berkuatkuasa. x. melaporkan masalah yang berlaku seperti spam dan pencerobohan kepada penyedia perkhidmatan media sosial.	Warga KNS

8-8 DATA TERBUKA
Open Data

Objektif: Data terbuka bertujuan meningkatkan kualiti dan ketelusan penyampaian perkhidmatan kerajaan menerusi perkongsian data yang tepat, cepat dan relevan selaras dengan inisiatif kerajaan.

8-8-1 Pengurusan Data Terbuka
Management of Open Data

Pengurusan data terbuka KNS perlu berasaskan tadbir urus dan aktiviti semasa yang berkuatkuasa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. mewujudkan Pasukan Kerja Data Terbuka untuk melaksanakan tugas dan aktiviti berkaitan. ii. melaksanakan pemantauan secara berkala berkaitan pelaksanaan data terbuka di bawah pentadbiran KNS.	Pasukan Kerja Data Terbuka

BIDANG 9

KESELAMATAN KOMUNIKASI

Communications Security

BIDANG 9
KESELAMATAN KOMUNIKASI
Communications Security

9-1 PENGURUSAN KESELAMATAN RANGKAIAN
Communications Security

Objektif: Memastikan kawalan keselamatan dan perlindungan maklumat termasuk kemudahan pemproses maklumat dalam rangkaian.

9-1-1 Kawalan Rangkaian
Network Controls

Infrastruktur rangkaian hendaklah dikawal dan diuruskan bagi memastikan matlamat kerahsiaan, integriti dan ketersediaan data/ maklumat tercapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. peralatan rangkaian hendaklah diletakkan di lokasi yang selamat. ii. perkakasan atau perisian keselamatan rangkaian hendaklah dipasang, dikonfigurasi dan diselia. iii. konfigurasi peralatan keselamatan rangkaian hendaklah dirancang, diluluskan dan direkodkan. iv. semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan jabatan. v. semua perisian penganalisa paket seperti *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO. vi. sebarang penyambungan rangkaian yang bukan di bawah kawalan jabatan adalah tidak dibenarkan. vii. penggunaan modem, *access point* dan *wireless broadband* persendirian hendaklah mendapat kebenaran ICTSO dan memaklumkan kepada pentadbir rangkaian.	Pengurus ICT dan Pentadbir Sistem ICT

9-1-2 Keselamatan Perkhidmatan Rangkaian *Security of Network Services*	
Pengurusan bagi semua perkhidmatan rangkaian dalaman atau *outsource* yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	ICTSO, Ketua Jabatan, Pentadbir Sistem ICT dan Pihak Luaran
9-1-3 Pengasingan Rangkaian *Segregation in Networks*	
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian pentadbiran KNS.	ICTSO, Ketua Jabatan dan Pentadbir Sistem ICT
9-2 PERPINDAHAN MAKLUMAT *Information Transfer*	
Objektif: Memastikan kawalan keselamatan semasa perpindahan atau pertukaran maklumat antara jabatan/ agensi dengan pihak luaran.	
9-2-1 Dasar dan Prosedur Kawalan Perpindahan Maklumat *Information Transfer Policies and Procedures*	
Perkara yang perlu dipatuhi adalah seperti yang berikut: i. polisi, prosedur atau kawalan pemindahan data/ maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data/ maklumat melalui sebarang jenis kemudahan komunikasi. ii. terma pemindahan data/ maklumat dan perisian antara pentadbiran KNS dengan pihak luaran perlu dimasukkan di dalam perjanjian. iii. media yang mengandungi maklumat perlu dilindungi. iv. memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Warga KNS dan Pihak Luaran

9-2-2 Pengurusan E-mel Elektronik *Electronic Email Management*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. pengguna e-mel di jabatan hendaklah mematuhi etika penggunaan e-mel dan internet merujuk dasar/ pekeliling semasa yang sedang berkuatkuasa. ii. hanya e-mel rasmi jabatan sahaja dibenarkan dalam setiap urusan rasmi. iii. sebarang pemindahan dokumen terperingkat melalui e-mel hendaklah merujuk kepada dasar/ pekeliling kriptografi yang sedang berkuatkuasa. iv. jabatan perlu menyediakan polisi, prosedur atau arahan-arahan bertulis yang bersesuaian mengenai penggunaan e-mel.	Pentadbir Sistem ICT dan Warga KNS
9-2-3 Kerahsiaan dan *Non-Disclosure Agreement (NDA)* *Confidentiality and Non-Disclosure Agreement (NDA)*	
Syarat-syarat perjanjian kerahsiaan atau *Non-Disclosure Agreement* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pihak luaran hendaklah bersetuju dan mematuhi semua keperluan keselamatan yang terkandung di dalam dokumen NDA.	ICTSO, Ketua Jabatan, Pentadbir Sistem ICT, Warga KNS dan Pihak Luaran

BIDANG 10

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

System Acquisition, Development and Maintenance

BIDANG 10
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM
System Acquisition, Development and Maintenance

10-1 KEPERLUAN KESELAMATAN SISTEM
Security Requirements of Information Systems

Objektif: Memastikan keperluan keselamatan sistem maklumat dikenal pasti, dipersetujui dan didokumenkan pada setiap peringkat perolehan, pembangunan, penambahbaikan dan penyelenggaraan. Pernyataan keperluan bagi sistem maklumat hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

10-1-1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat
Information Security Requirements Analysis and Specifications

Perkara yang perlu dipatuhi adalah seperti berikut: i. perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambilkira kawalan keselamatan bagi memastikan tiada ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. ii. ujian keselamatan hendaklah dijalankan ke atas sistem aplikasi untuk pengesahan dan memastikan integriti data. iii. sistem aplikasi perlu mematuhi semakan pengesahan berdasarkan V&V (*validation and verification*). iv. pengujian secara menyeluruh bagi semua sistem aplikasi hendaklah dilaksanakan bagi memastikan sistem berkenaan mematuhi aspek keselamatan yang telah ditetapkan.	ICTSO, Pentadbir Sistem Aplikasi dan Pemilik Sistem

10-2 KESELAMATAN PEMBANGUNAN SISTEM DAN PROSES SOKONGAN
Security in System Development and Support Services

Objektif: Memastikan keperluan keselamatan sistem maklumat dikenal pasti, dipersetujui dan didokumenkan pada setiap kitaran hayat pembangunan sistem aplikasi.

10-2-1 Dasar Selamat Pembangunan Sistem
System Development Secure Policy

Peraturan atau tatacara pembangunan sistem aplikasi hendaklah diwujudkan dan digunakan oleh jabatan/ agensi. Perkara yang perlu dipatuhi adalah seperti berikut: i. keperluan keselamatan maklumat semasa persekitaran kitaran hayat pembangunan. ii. panduan keselamatan dalam kitar hayat pembangunan sistem maklumat. iii. keselamatan maklumat dalam fasa reka bentuk. iv. pemeriksaan keselamatan dalam perkembangan projek. v. keselamatan repositori atau ruang storan. vi. keselamatan dalam kawalan versi. vii. keperluan pengetahuan keselamatan dalam pembangunan sistem aplikasi. viii. kebolehan mengenal pasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem aplikasi.	Pentadbir Sistem Aplikasi dan Pemilik Sistem

10-2-2 Prosedur Kawalan Perubahan Sistem
System Change Control Procedures

Perubahan ke atas sistem aplikasi di dalam kitaran pembangunan hendaklah dikawal menggunakan prosedur kawalan perubahan. Perkara yang perlu dipatuhi adalah seperti berikut: i. penambahbaikan atau pengubahsuaian ke atas fungsi atau modul sistem aplikasi hendaklah diuji, direkod dan disahkan sebelum digunapakai.	Pemilik Sistem dan Pentadbir Sistem Aplikasi

ii. melaksanakan pengemaskinian ke atas perisian yang digunakan mengikut keperluan. iii. mengawal kawalan versi sistem mengikut keperluan jabatan/ agensi. iv. mengkaji impak operasi dan keselamatan maklumat bagi setiap perubahan yang dicadangkan. v. melaksanakan perubahan sistem pada pelayan pembangunan untuk menguji keberkesanan operasi. vi. setiap permohonan perubahan/ penambahbaikan sistem hendaklah menggunakan Change Request Form (CRF) bagi memantau dan mengawal perubahan/ penambahbaikan yang dilaksanakan oleh pengaturcara. vii. kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	
10-2-3 Kajian Semula Teknikal Aplikasi Selepas Perubahan Platform Operasi *Technical Review of Applications After Operating Platform Changes*	
Perubahan platform operasi sama ada sistem pengoperasian atau rangka kerja (*framework*) hendaklah dikaji dan diuji bagi memastikan tiada sebarang masalah yang timbul terhadap operasi atau keselamatan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan perubahan platform operasi ini dilaksanakan dalam persekitaran pengujian. ii. kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform operasi. iii. perubahan platform dimaklumkan dari semasa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. iv. memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.	Pemilik Sistem dan Pentadbir Sistem ICT

10-2-4 Prinsip Kejuruteraan Sistem yang Selamat *Secure System Engineering Principles*	
Prinsip kejuruteraan yang selamat bagi pembangunan sistem maklumat hendaklah diwujudkan, di dokumentasi, di selenggara dan diguna pakai dalam pelaksanaan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: i. memastikan keselamatan seperti ancaman daripada bencana alam dan manusia diambil kira. ii. perlindungan maklumat dalam pembangunan sistem semasa pemprosesan, perpindahan dan penyimpanan. iii. mengambil kira kriteria di bawah dalam prinsip kejuruteraan pembangunan system seperti berikut: a. *business layer* - berdasarkan tahap pengesahan pengguna; hanya pengguna tertentu boleh melihat data peribadi. b. *data layer* - hanya log masuk dengan kata laluan pangkalan data yang selamat untuk aktiviti penyelenggaraan pangkalan data dibenarkan. c. *application layer* - penggunaan enkripsi untuk penghantaran maklumat. d. *technology layer* - penggunaan perisian sumber terbuka dan infrastruktur rangkaian.	Pemilik Sistem dan Pentadbir Sistem Aplikasi
10-2-5 Keselamatan Persekitaran Pembangunan Sistem *Secure Development Environment*	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*system development life cycle*). Antara perkara yang perlu diberi perhatian adalah seperti berikut: i. memastikan persekitaran pembangunan sistem yang berbeza diasingkan dan mewujudkan mekanisme kawalan. ii. capaian ke persekitaran pembangunan ini hanya kepada pengguna yang dibenarkan sahaja. iii. memastikan pembangunan sistem menggunakan mekanisme yang selamat dalam perpindahan data atau maklumat.	Pentadbir Sistem Aplikasi dan Pemilik Sistem

10-2-6 Pembangunan Perisian oleh Pihak Luaran *Outsourced Software Development*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. pembangunan sistem secara *outsource* perlu diselia dan dipantau oleh pentadbir dan pemilik sistem jabatan/ agensi. ii. memastikan perpindahan teknologi oleh pihak luaran kepada jabatan/ agensi dilaksanakan. iii. kod sumber bagi sistem aplikasi merupakan hak milik jabatan/ agensi dan boleh diakses serta boleh dibuat perubahan oleh jabatan/ agensi. iv. memastikan pembangunan sistem menggunakan teknik *secure coding* dan *cross platform.* v. semua capaian yang dibenarkan kepada pihak luaran hendaklah mengikut keperluan jabatan/ agensi. vi. pihak luaran hendaklah menyediakan dokumentasi lengkap sistem mengikut keperluan dan tempoh yang telah ditetapkan oleh jabatan/ agensi. vii. pihak luaran perlu melaksanakan ujian keselamatan terhadap sistem aplikasi sebelum menyerahkan kepada pihak kerajaan.	Pengurus ICT, Pentadbir Sistem Aplikasi dan Pemilik Sistem
10-2-7 Pengujian Keselamatan Sistem *System Security Testing*	
Perkara yang perlu diberi perhatian adalah seperti berikut: i. pengujian fungsi keselamatan sistem aplikasi hendaklah dilaksanakan semasa fasa pembangunan. ii. semua sistem baharu atau penambahbaikan sistem hendaklah menjalani ujian keselamatan. iii. Sekiranya pembangunan sistem dilaksanana secara luaran (outsourced), pengujian keselamatan perlu dilaksanakan oleh pihak ketiga selain pembekal yang dilantik.	Pemilik Sistem dan Pentadbir Sistem Aplikasi

10-2-8 Pengujian Penerimaan Sistem *System Accepting Testing*	
Perkara yang perlu diberi perhatian adalah seperti berikut: i. pembangunan dan penambahbaikan sistem aplikasi hendaklah memenuhi spesifikasi yang ditetapkan sebelum diterima pakai. ii. pembangunan dan penambahbaikan sistem aplikasi perlu melalui peringkat pengujian *User Acceptance Test* (UAT), *Provisional Acceptance Test* (PAT) & *Final Acceptance Test* (FAT) sebelum dilaksanakan. iii. dokumentasi sistem aplikasi perlu disediakan dan dikemaskini mengikut kawalan versi.	Pentadbir Sistem Aplikasi, Pemilik Sistem dan Pengguna
10-3 DATA UJIAN *Test Data*	
Objektif: Memastikan keselamatan data semasa pengujian.	
10-3-1 Perlindungan Data Ujian *Protection of Test Data*	
Antara perkara yang boleh diberi perhatian adalah seperti berikut: i. data ujian yang digunakan hendaklah bersesuaian mengikut keperluan sistem. ii. penggunaan data ujian hendaklah dilaksanakan ke atas kod sumber yang terkini. iii. data ujian perlu dihapuskan setelah proses pengujian dilaksanakan.	Pemilik Sistem dan Pentadbir Sistem Aplikasi

BIDANG II

HUBUNGAN PIHAK LUARAN

Supplier Relationship

BIDANG 11
HUBUNGAN PIHAK LUARAN
Supplier Relationship

11-1 KESELAMATAN MAKLUMAT PERHUBUNGAN DENGAN PIHAK LUARAN
Information Security in Supplier Relationships

Objektif: Memastikan kawalan keselamatan ke atas aset ICT yang boleh dicapai oleh pihak luaran.

11-1-1 Dasar Keselamatan Maklumat Pihak Luaran
Information Security Policy for Supplier Relationships

Antara perkara yang boleh diberi perhatian adalah seperti berikut: a) memastikan perjanjian disediakan mengikut tatacara perolehan yang berkuatkuasa. b) pihak luaran perlu mematuhi semua peraturan keselamatan yang berkuatkuasa seperti capaian ke atas aplikasi, aset dan premis kerajaan. c) memastikan pihak luaran diberikan taklimat keselamatan dan menandatangani Surat Akuan Pematuhan PKS Pentadbiran KNS seperti di **Lampiran 1** dan dokumen *Non-Disclosure Aggreement* (NDA). d) memastikan pihak luaran melaksanakan tapisan keselamatan melalui Sistem e-Vetting yang disediakan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO). e) menandatangani Perakuan Untuk Ditandatangani Komuniti Keselamatan Atau Mana-Mana Pihak Lain Yang Berurusan Dengan Perkhidmatan Awam Atau Yang Berkhidmat Di Kediaman Rasmi Kerajaan Berkaitan Dengan Akta Rahsia Rasmi 1972 [Akta 88] seperti di **Lampiran 3.**	ICTSO, Pengurus ICT Pentadbir Sistem ICT dan Pihak Luaran

11-1-2 Menangani Aspek Keselamatan dalam Perjanjian Pembekal *Addressing Security Within Supplier Agreements*	
Keperluan keselamatan maklumat hendaklah diwujudkan dan dipersetujui dengan pembekal yang akan mengakses, memproses, menyimpan, berkomunikasi atau menyediakan komponen infrastruktur di pentadbiran KNS. Perkara yang perlu diambil kira seperti berikut: i. mengadakan sesi taklimat keselamatan. ii. mengklasifikasikan maklumat. iii. keperluan undang-undang dan peraturan yang sedang berkuat kuasa. iv. obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan. v. tapisan keselamatan pihak luaran. vi. tindakan undang-undang.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
11-2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK LUARAN *Supplier Service Delivery Management*	
Objektif: Mengekalkan tahap keselamatan maklumat dalam penyampaian perkhidmatan selaras dengan perjanjian bersama pihak luaran.	
11-2-1 Memantau dan Mengkaji Semula Perkhidmatan Pembekal *Monitoring and Review of Supplier Services*	
Perkara yang perlu dipatuhi seperti berikut: i. melaksanakan pemantauan terhadap perkhidmatan mengikut keperluan termasuk penilaian tahap prestasi perkhidmatan. ii. memantau tahap prestasi perkhidmatan untuk mengesahkan pihak luaran mematuhi perjanjian. iii. menyemak dan mengesahkan laporan perkhidmatan serta laporan insiden keselamatan yang dikemukakan oleh pihak luaran berdasarkan kepada status kemajuan perkhidmatan.	Pengurus ICT dan Pentadbir Sistem ICT

11-2-2 Pengurusan Perubahan dalam Perkhidmatan Pihak Luaran *Managing Changes to Supplier Services*	
Perkara yang perlu dipatuhi seperti berikut: i. memastikan perubahan dalam perkhidmatan pihak luaran dipersetujui bersama dan mendapat kelulusan pengurusan. ii. memastikan perubahan dalam perjanjian dengan pihak luaran mengambil kira maklumat kritikal sistem, proses yang terlibat dan kajian risiko. iii. perubahan yang dilakukan untuk meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur. iv. perubahan dalam perkhidmatan pihak luaran adalah seperti peningkatan teknologi, rangkaian, produk, perkakasan atau perubahan lokasi.	ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Luaran

BIDANG 12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Information Security Incident Management

BIDANG 12
PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT
Information Security Incident Management

12-1 PENGURUSAN INSIDEN KESELAMATAN DAN PENAMBAHBAIKAN
Management of Information Security Incidents and Improvements

Objektif: Memastikan pendekatan yang konsisten dan berkesan untuk pengurusan insiden keselamatan maklumat termasuk mengenal pasti ancaman dan kelemahan.

12-1-1 Tanggungjawab dan Prosedur
Responsibilities and Procedures

Perkara yang perlu dipatuhi seperti berikut: i. memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan. ii. pemakluman kepada pihak berkuasa atau agensi yang bertanggungjawab dalam menangani insiden keselamatan mengikut keperluan.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

12-1-2 Pelaporan Insiden Keselamatan
Reporting Information Security Events

Insiden keselamatan ICT bermaksud musibah (*adverse event*) atau ancaman kemungkinan berlaku ke atas aset ICT secara sengaja atau tidak. Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO atau CSIRTNS dengan kadar segera apabila berlakunya perkara seperti berikut: i. maklumat didapati hilang atau disyaki hilang kepada pihak yang tidak bertanggungjawab. ii. maklumat didapati didedahkan atau disyaki didedahkan kepada pihak yang tidak diberi kuasa capaian. iii. sistem aplikasi digunakan tanpa kebenaran atau disyaki sedemikian.	ICTSO, CSIRTNS dan Warga KNS

iv. kawalan akses hilang, dicuri, diseleweng, didedahkan atau disyaki sedemikian. v. berlaku insiden pada sistem aplikasi atau sistem rangkaian yang luar daripada kebiasaan. vi. aduan dan laporan insiden keselamatan ICT boleh dibuat kepada ICTSO dan CSIRTNS dengan merujuk proses kerja pelaporan insiden yang sedang berkuatkuasa.	
12-1-3 Penilaian dan Analisa Aktiviti Keselamatan Maklumat *Assessment of and Decision on Information Security Events*	
Aktiviti yang memberi ancaman kepada keselamatan maklumat hendaklah dinilai dan dianalisa sama ada akan diklasifikasikan sebagai insiden atau tidak. Perkara yang perlu diambil kira adalah seperti berikut: i. merekod dan menyimpan semua aktiviti keselamatan maklumat secara berpusat atau pada peralatan ICT. ii. menganalisa setiap aktiviti keselamatan maklumat secara berkala bagi memastikan pihak yang berkaitan dapat mengklasifikasikan aktiviti tersebut.	ICTSO, Pengurus ICT, dan Pentadbir Sistem ICT
12-1-4 Tindak Balas Terhadap Insiden Keselamatan Maklumat *Response to Information Security Incidents*	
Perkara yang perlu diambil kira adalah seperti berikut: i. mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku. ii. menjalankan kajian dan analisa. iii. menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin. iv. menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti. v. menyalin dan merekodkan semua bahan bukti. vi. maklumat aktiviti penyalinan. vii. menangani insiden keselamatan maklumat mengikut proses kerja pengendalian insiden yang sedang berkuatkuasa.	ICTSO, CSIRTNS, Pengurus ICT, dan Pentadbir Sistem ICT

12-1-5 Pengalaman dari Insiden Keselamatan Maklumat *Learning from Information Security Incidents*	
Pengalaman serta pengetahuan yang diperolehi melalui proses menganalisis dan penyelesaian insiden keselamatan maklumat yang telah berlaku boleh digunakan untuk mengurangkan kebarangkalian (*likelihood*) atau kesan insiden pada masa akan datang. Perkara yang perlu diambil kira adalah seperti berikut: i. menyimpan dan merekodkan tindakan pengukuhan yang telah dilaksanakan semasa berlaku insiden keselamatan. ii. menganalisa impak ke atas tindakan yang dilaksanakan.	ICTSO, CSIRTNS, Pengurus ICT dan Pentadbir Sistem ICT
12-1-6 Pengumpulan Bahan Bukti ***Collection of Evidence***	
Perkara yang perlu diambil kira adalah seperti berikut: i. prosedur untuk mengenal pasti, mengumpul, mendapatkan dan menyimpan bahan bukti hendaklah dibangunkan bagi memastikan bahan bukti dilindungi dan tersedia. ii. menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti.	ICTSO, CSIRTNS, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG 13

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Business Continuity Management

BIDANG 13
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN
Business Continuity Management

13-1 KESINAMBUNGAN KESELAMATAN MAKLUMAT
Information Security Continuity

Objektif: Memastikan aspek keselamatan maklumat diberi perhatian dan dimasukkan dalam sistem pengurusan kesinambungan perkhidmatan.

13-1-1 Perancangan Kesinambungan Keselamatan Maklumat
Information Security Continuity Planning

Jabatan/ Agensi hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat semasa berlaku krisis dan bencana yang boleh memberi gangguan kepada sistem penyampaian kerajaan. Perkara yang perlu diambil kira adalah seperti berikut: i. membangunkan Pelan Kesinambungan Perkhidmatan (PKP) dengan mengenal pasti aspek keselamatan maklumat yang terlibat. ii. melaksanakan *post-mortem* dan mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal jabatan/ agensi. iii. mengemas kini struktur tadbir urus PKP Jabatan/ Agensi jika berlaku pertukaran pegawai. iv. memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP. v. memastikan pelan diluluskan oleh pegawai yang bertanggungjawab.	Pasukan PKP

13-1-2 Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat *Verify, Review and Evaluate Information Security Continuity*	
Jabatan/ Agensi hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pasukan PKP
13-2 LEWAHAN *Redundancy*	
Objektif: Memastikan ketersediaan perkhidmatan dan kemudahan pemprosesan atau sistem maklumat.	
13-2-1 Ketersediaan Perkhidmatan/ Kemudahan Pemprosesan Maklumat *Availability of Information Process Facilities*	
Kemudahan pemprosesan maklumat jabatan/ agensi perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji *(failover test)* keberkesanannya dari semasa ke semasa.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

BIDANG 14

PEMATUHAN

Compliance

BIDANG 14
PEMATUHAN
Compliance

14-1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN KONTRAK
Compliance with Legal and Contractual Requirements

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

14-1-1 Mengenal Pasti Keperluan Perundangan dan Perjanjian Kontrak
Compliance with Legal and Contractual Requirements

Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan jabatan/ agensi perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat.	Warga KNS

14-1-2 Perlindungan Rekod
Protection of Records

Rekod sama ada digital atau bukan digital hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak dan keperluan jabatan/ agensi. Perkara yang perlu diberi perhatian adalah seperti berikut: i. penyimpanan, pengendalian dan pelupusan rekod. ii. jadual penyimpanan rekod. iii. inventori rekod.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

14-1-3 Privasi dan Perlindungan Maklumat Peribadi
Privacy and Protection of Personally Identifiable Information

Jabatan/ Agensi perlu mengenal pasti privasi serta melindungi maklumat peribadi pengguna seperti yang tertakluk dalam undang - undang dan peraturan yang berkenaan. Perkara yang boleh diberi perhatian adalah seperti berikut:	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

i. tidak mendedahkan maklumat peribadi pengguna pada mana-mana pihak yang tidak berkaitan. ii. memastikan kawalan penyimpan rekod maklumat peribadi pengguna di tempat yang selamat. iii. maklumat peribadi pengguna hanya boleh digunakan untuk tujuan rasmi dengan kebenaran.	
14-1-4 Peraturan Kawalan Kriptografi *Regulation of Cryptographic Controls*	
Jabatan/ Agensi perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan yang sedang berkuatkuasa. Perkara yang perlu diberi perhatian adalah seperti berikut: i. sekatan ke atas pembekal perkakasan dan perisian komputer yang melaksanakan atau mengubahsuai fungsi kriptografi tanpa kelulusan pihak kerajaan/ berkuasa. ii. sekatan penggunaan enkripsi yang tidak dibenarkan. iii. mematuhi kaedah akses yang dibenarkan bagi maklumat enkripsi perkakasan dan perisian dengan merujuk dokumen Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) dan peraturan yang sedang berkuatkuasa.	CIO/ CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
14-2 KAJIAN KESELAMATAN MAKLUMAT *Information Security Reviews*	
Objektif: Memastikan keselamatan maklumat dilaksanakan dan beroperasi selaras dengan polisi atau prosedur jabatan/ agensi.	
14-2-1 Kajian Keselamatan Maklumat oleh Pihak Ketiga atau Badan Bebas *Independent Review of Information Security*	
Jabatan/ Agensi perlu memastikan kaedah pengurusan keselamatan maklumat serta pelaksanaannya seperti objektif kawalan, kawalan, polisi dan prosedur dikaji secara bebas oleh pihak luaran sekiranya diperlukan.	CIO/ CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

14-2-2 Pematuhan kepada Dasar Keselamatan dan Standard *Compliance with Security Policies and Standards*	
Perkara yang perlu diberi perhatian adalah seperti berikut: i. memastikan kajian ke atas pematuhan dan prosedur pemprosesan maklumat di dalam bidang tanggungjawab mereka selaras dengan dasar keselamatan maklumat atau lain-lain keperluan keselamatan. ii. mengenal pasti punca-punca ketidakpatuhan. iii. menilai keperluan tindakan untuk mencapai pematuhan. iv. melaksanakan tindakan pembetulan yang sewajarnya. v. mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti kekurangan serta kelemahan untuk penambahbaikan. vi. Semua warga KNS hendaklah membaca, memahami dan mematuhi PKS Pentadbiran KNS, undang-undang atau peraturan lain yang berkaitan yang berkuat kuasa.	CIO/ CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
14-2-3 Pematuhan Kajian Teknikal ***Technical Compliance Review***	
Sistem maklumat hendaklah dikaji mengikut keperluan supaya selaras dengan pematuhan dasar dan standard.	CIO/ CDO, ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

GLOSARI

ISTILAH	KETERANGAN
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset Alih	Aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bantuan.
Aset ICT	Terdiri daripada perkakasan, perisian, aplikasi sistem, perkhidmatan, data, maklumat, manusia, media storan, dokumentasi, premis komputer dan peralatan rangkaian.
AVR	Automatic Voltage Regulator (AVR) atau pengatur voltan automatik ialah peranti elektronik yang mengekalkan paras voltan malar kepada peralatan elektrik pada beban yang sama. AVR mengawal variasi voltan untuk menyampaikan bekalan kuasa yang berterusan dan boleh dipercayai.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur Lebar - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
Biometrik	Kaedah yang digunakan untuk pengecaman identiti individu melalui pengesanan seperti cap jari, suara dan retina.
CAPTCHA	*Completely Automated Public Turing test to tell Computers and Humans Apart* bertujuan untuk membezakan antara mesin (bot) dan manusia.

CCTV	*Closed-Circuit Television* – Sistem TV yang digunakan secara komersial di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
Clear Desk dan *Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
CSIRTNS	*Cyber Security Incident Response Team* Negeri Sembilan. Pasukan yang ditubuhkan untuk mengendalikan insiden keselamatan siber di bawah Pentadbiran Kerajaan Negeri Sembilan.
CIO/CDO	*Chief Information Officer/Chief Digital Officer* – Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Cross Platform	Boleh digunakan dengan pelbagai jenis sistem pengoperasian komputer seperti Windows, Mac OS, Linux dan Solaris.
CyberStalking/ *CyberHarassment*	Penggunaan Internet atau cara elektronik lain untuk mengintai atau mengganggu individu, kumpulan atau organisasi. Contoh aktiviti adalah termasuk tuduhan palsu, fitnah, kecurian identiti, ancaman, vandalisme dan lain-lain.
Denial of Service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Disaster Recovery Centre (DRC)	Lokasi alternatif fizikal yang menggantikan pusat operasi utama jika berlaku bencana. *Disaster Recovery Centre* (DRC) dilengkapi dengan perkakasan, perisian, sistem aplikasi dan sistem rangkaian yang menyerupai pusat operasi utama.

Disaster Recovery Plan (DRP)	Dokumen rasmi yang mengandungi arahan terperinci tentang cara bertindak balas terhadap insiden yang tidak dirancang seperti bencana alam, gangguan bekalan elektrik, serangan siber dan lain-lain. Pelan itu mengandungi strategi untuk meminimumkan kesan bencana, membantu organisasi meneruskan kesinambungan perkhidmatan kepada capaian pengguna.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Final Acceptance Test (FAT)	Ujian Penerimaan Akhir (FAT) adalah penilaian yang dilakukan semasa fasa pentauliahan oleh pihak ketiga yang melibatkan keseluruhan projek bagi menentukan prestasi dan keupayaan projek sebelum diguna pakai.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan – Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hacking Tool	Program yang direka untuk membantu penggodaman, atau yang boleh digunakan untuk tujuan penggodaman.

Hard Disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu *port*kepada semua *port*yang lain.
ICTSO	*ICT Security Officer* - Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Idle	Keadaan atau sesuatu yang tidak aktif.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh

	bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Kawasan Larangan	Kawasan yang dihadkan kemasukan kepada pegawai-pegawai tertentu sahaja. Ini dilaksanakan untuk melindungi Aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan adalah seperti berikut: i. Bilik YAB Menteri Besar ii. Bilik YB SUK iii. Bilik EXCO iv. Bilik Timbalan SUK v. Dewan Undangan Negeri vi. Bilik Dato' Bandar/ Pegawai Daerah/ Yang Dipertua vii. Bilik Ketua Jabatan/ Bahagian/ Unit viii. Pusat Data/ Bilik *Server* ix. Bilik Kawalan/ Peralatan Keselamatan x. Bilik Penyimpanan Media xi. Bilik Kebal xii. Disaster Recovery Centre (DRC) xiii. Kawasan yang berisiko
Kriptografi	Kaedah untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
*Local Area Network (*LAN)	Koleksi peranti yang disambungkan bersama dalam satu lokasi fizikal, seperti bangunan, pejabat atau rumah.
Logout	*Log-out* komputer – Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Media Tandatangan Digital	Satu mekanisma yang digunakan untuk menandatangani sesuatu dokumen rasmi secara elektronik.

Mobile Code	Merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya sebagai pelayar internet.
MODEM	MOdulator DEModulator - Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Network Analyzer	Alat yang digunakan untuk mengenal pasti peranti atau bahagian rangkaian yang menyebabkan kesesakan aliran trafik.
Outsource	Menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pegawai Aset	Pegawai yang dilantik untuk menjaga dan menguruskan aset.
Pegawai Keselamatan Jabatan	Pegawai yang bertanggungjawab mengenai pentadbiran Jabatan/Agensi untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan
Pembangun Sistem	Individu atau beberapa individu yang bertanggungjawab membangunkan suatu sistem perkomputeran. Tugas yang dilaksanakan merangkumi analisis, reka bentuk, pembangunan, pelaksanaan, pengujian dan penyelenggaraan sistem.
Pemilik Sistem	Individu atau organisasi yang bertanggungjawab untuk pembangunan, perolehan, penyepaduan, pengubahsuaian, operasi dan penyelenggaraan, dan/atau pelupusan akhir sistem maklumat.

Pengguna	Pegawai dan kakitangan yang bertanggungjawab menggunakan sistem.
Pengujian Keselamatan	Proses menilai dan menguji keselamatan maklumat perkakasan, perisian, rangkaian atau persekitaran sistem ICT bertujuan menyemak dan memperakui tahap keselamatan aset atau kemudahan ICT.
Pengkomputeran Awan	Perkhidmatan perkongsian sumber ICT secara virtual tanpa penyediaan infrastruktur di pihak pengguna yang membolehkan capaian melalui rangkaian kepada himpunan sumber pengkomputeran yang fleksibel dan elastik dengan cara perkongsian sumber bersama, sama ada secara fizikal atau maya dengan keupayaan pembekalan secara layan diri dan / atau pengurusan oleh pihak ketiga mengikut permintaan pengguna.
Pengurus ICT	Pegawai yang bertanggungjawab menguruskan keselamatan ICT di bawah kawalannya.
Pentadbiran Kerajaan Negeri Sembilan	Semua Jabatan Negeri termasuk Badan Berkanun Negeri dan Pihak Berkuasa Tempatan.
Pentadbir Sistem ICT	Pegawai yang bertanggungjawab sebagai Pentadbir Rangkaian dan Keselamatan/ Pentadbir Sistem Aplikasi/ Pentadbir Laman Web (Webmaster)/ Pentadbir Pangkalan Data, Pentadbir Pusat Data dan Pentadbir E-mel.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Pihak Luaran	Terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang terlibat dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan.

Pelan Kesinambungan Perkhidmatan (PKP)	Pelan bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama agensi dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.
Provisional Acceptance Test (PAT)	Fasa Ujian Penerimaan Sementara adalah penerimaan bersyarat yang bermaksud bahawa pengguna telah menerima projek tetapi prestasi perlu disahkan atau disahkan dalam tempoh yang telah dipersetujui.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Restoration	Pemulihan ke atas data.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer sekiranya tidak digunakan dalam jangka masa tertentu.
Secure Coding	Amalan membangunkan perisian komputer, sistem aplikasi dengan cara selamat bagi membantu mengurangkan atau menghapuskan kelemahan dalam perisian/ sistem sebelum sesuatu perisian/sistem digunakan.
Sniffer	Perisian atau perkakasan yang membolehkan pengguna memantau trafik internet dan merekod aliran data di dalam rangkaian.
Secure Socket Layer (SSL)	Protokol kriptografi yang digunakan dalam keselamatan komunikasi melalui internet.

Server	Program atau peranti komputer yang menyediakan perkhidmatan kepada program komputer lain dan penggunanya.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
User Acceptance Test (UAT)	Fasa pembangunan sistem aplikasi/ perisian di mana sistem aplikasi/ perisian tersebut diuji dalam "dunia nyata" oleh pengguna.
V&V	V&V (*validation and verification*) ialah satu prosedur bebas yang digunakan untuk menyemak sama ada komponen, produk, perkhidmatan atau sistem memenuhi keperluan dan spesifikasi yang ditetapkan dan ia memenuhi tujuan keseluruhan yang dimaksudkan.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

Wide Area Network (WAN)	Rangkaian yang merangkumi kawasan yang luas.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER (PKS)
PENTADBIRAN KERAJAAN NEGERI SEMBILAN
VERSI 1.0

Nama (huruf besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan/Agensi/Bahagian/Unit : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

Tandatangan : .....

Tarikh : .....

Pengesahan

.....

Chief Digital Officer (CDO)/
Chief Information Officer (CIO)/
Ketua Jabatan

LAMPIRAN 2

PERAKUAN UNTUK DITANDATANGANI OLEH PENJAWAT AWAM BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan:.....

Nama dengan Huruf Besar:.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Agensi:.....

Tarikh:.....

Disaksikan oleh:.....
(Tandatangan)

Nama dengan Huruf Besar:.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Agensi:.....

Tarikh:.....

Cop Jabatan:.....

LAMPIRAN 3

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

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

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

Tandatangan:.....

Nama (huruf besar):.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Organisasi:.....

Tarikh:.....

Disaksikan oleh:.....
(Tandatangan)

Nama (huruf besar):.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Organisasi:.....

Tarikh:.....

Cop Jabatan:.....

LAMPIRAN 4

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

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

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

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

Tandatangan:.....

Nama (huruf besar):.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Organisasi:.....

Tarikh:.....

Disaksikan oleh:.....
(Tandatangan)

Nama (huruf besar):.....

No. Kad Pengenalan:.....

Jawatan:.....

Jabatan/ Organisasi:.....

Tarikh:.....

Cop Jabatan:.....

SENARAI PERATURAN DAN UNDANG-UNDANG

AKTA/ PEKELILING/ SURAT ARAHAN/ DASAR/ POLISI/ GARIS PANDUAN
Surat Akujanji
Arahan Perbendaharaan
Pekeliling Perbendaharaan Malaysia
Perintah-Perintah Am
Akta Rahsia Rasmi 1972
Akta Tandatangan Digital 1997
Akta Jenayah Komputer 1997
Akta Hak Cipta (Pindaan) Tahun 1997
Akta Komunikasi dan Multimedia 1998
Arahan Teknologi Maklumat 2007
Arahan Keselamatan (Semakan & Pindaan 2017)
Pelan Kesenimbungan Perkhidmatan (PKP) Agensi/ Jabatan
Pelan Pemulihan Bencana/ *Disaster Recovery Plan* Jabatan/ Agensi
Polisi E-mel Rasmi Pentadbiran Kerajaan Negeri Sembilan
Garis Panduan Pengurusan Projek ICT Pentadbiran Kerajaan Negeri Sembilan
Garis Panduan Permohonan Kelulusan Teknikal dan Pelaporan Kemajuan Projek ICT Pentadbiran Kerajaan Negeri Sembilan
Garis Panduan Perkhidmatan Pengkomputeran Awan Pentadbiran Kerajaan Negeri Sembilan (NSGovCloud) Versi 1.0
Polisi Keselamatan Siber Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000
Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)

Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002 bertarikh 15 Januari 2002
Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
Garis Panduan Keselamatan MAMPU 2004
Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005
Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006
Pekeliling Perbendaharaan Bil. 5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaan
Surat Pekeliling Perbendaharaan Bil.2 Tahun 1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; (Dibatalkan oleh SPP 5/2007)
Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007
Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009
Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007
Surat Pekeliling Perbendaharaan Bil. 3 Tahun 1995 - Peraturan Perolehan Perkhidmatan Perundingan
Surat Arahan Ketua Pengarah MAMPU – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-Agensi Kerajaan yang bertarikh 23 Mac 2009
Surat Arahan Ketua Pengarah MAMPU - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam bertarikh 22 Jan 2010
Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010
Pekeliling Kemajuan Pentadbiran Awam Bilangan 3 Tahun 2015 – Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]
Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 – Panduan Pengurusan Pejabat bertarikh 30 April 2007

Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) bertarikh 19 November 2009 – Penggunaan Media Jaringan Sosial di Sektor Awam
Pelaksanaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 November 2010
Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 November 2010
Surat Arahan Ketua Pengarah Perkhidmatan Awam – Tindakan Ke Atas Penjawat Awam Yang Mendedahkan/Membocorkan Dokumen/Maklumat Terperingkat Kerajaan yang bertarikh 28 Januari 2015
Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam
Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) Versi 1.0, April 2016
Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team* (GCERT) oleh NACSA bertarikh 28 Januari 2019
Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022
Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022

UNIT PENGURUSAN TEKNOLOGI MAKLUMAT
Tingkat 3, Blok B, Wisma Negeri,
70503 Seremban,
Negeri Sembilan Darul Khusus
Tel: 06-7659011
Faks: 06-7627760
E-Mel: pentadbiranuptm@ns.gov.my
Portal: https://www.ns.gov.my