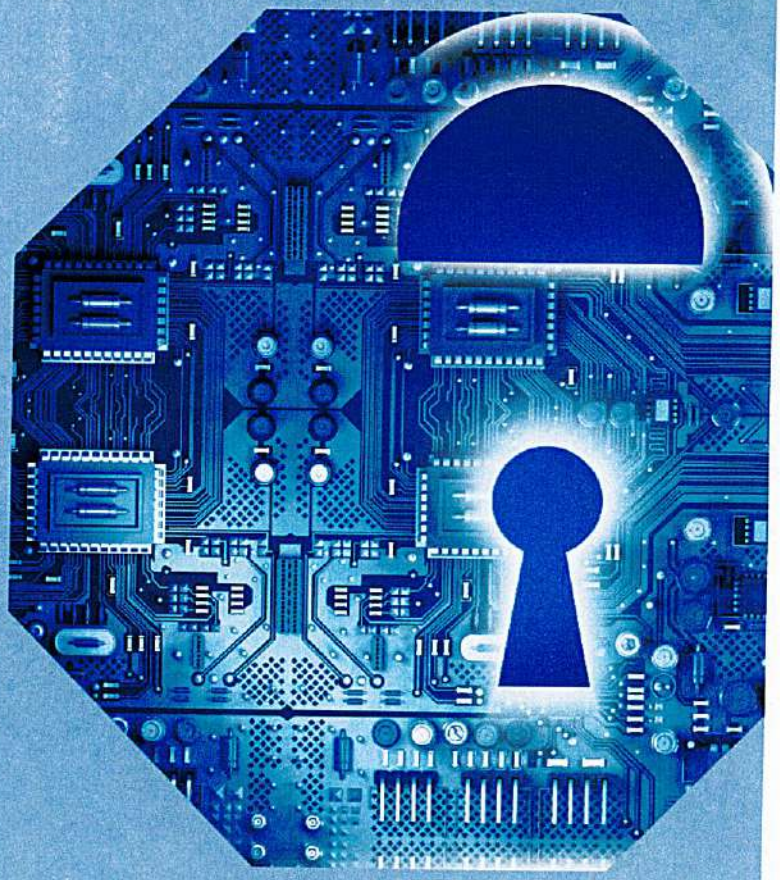
INSTITUT TANAH DAN UKUR NEGARA
KEMENTERIAN SUMBER ASLI DAN KELESTARIAN ALAM

POLISI
KESELAMATAN SIBER

Versi 2.0



POLISI KESELAMATAN SIBER

VERSI 2.0

DILULUSKAN OLEH :

.....

(KHAIRIN NAZRY BIN KARIM)

PENGARAH

INSTITUT TANAH DAN UKUR NEGARA

TARIKH :

15 Ogos 2025.

KANDUNGAN

SEJARAH DOKUMEN POLISI KESELAMATAN SIBER

VERSI	KELULUSAN	TARIKH KUAT KUASA
1.0	Mesyuarat JPICT INSTUN	31 Julai 2019
1.1	Mesyuarat JPICT INSTUN	10 Nov 2022
1.2	Mesyuarat Pengurusan INSTUN Bil.11/2024	11 Julai 2024
2.0	Mesyuarat Pengurusan INSTUN Bil.14/2025	15 Ogos 2025

SINGKATAN DAN TAKRIFAN

BCM	*Business Continuity Management*
BCP	*Business Continuity Plan*
BPK	Bahagian Pentadbiran dan Kewangan
BTM	Bahagian Teknologi Maklumat
CCP	*Communication Crisis Plan* / Pelan Krisis Komunikasi
CERT	*Computer Emergency Response Team*
CDO	*Chief Digital Officer*
CGSO	*Chief Government Security Office* / Pejabat Ketua Pegawai Keselamatan Kerajaan
CSIRT	*Cyber Security Incident Response Team*
DDOS	*Distributed Denial of Service*
DRP	*Disaster Recovery Plan* / Pelan Pemulihan Bencana
DRC	*Disaster Recovery Centre* / Pusat Pemulihan Bencana
ERP	*Emergency Response Planning* / Pengurusan Tindakbalas Kecemasan
ICT	*Information and Communication Technology*
ICTSO	*Information and Communication Technology Security Officer*
ID	*Identity*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
ISMP	*Information Security Management Plan* / Pelan Pengurusan Keselamatan Maklumat
ISMS	*Information Security Management System* / Sistem Pengurusan Keselamatan Maklumat
INSTUN	Institut Tanah dan Ukur Negara
JDN	Jabatan Digital Negara
JPICT	Jawatankuasa Pemandu ICT
JKOICT	Jawatankuasa Keselamatan dan Operasi ICT

KSU	Ketua Setiausaha
KJ	Ketua Jabatan
LAN	*Local Area Network*
NRES	Kementerian Sumber Asli dan Kelestarian Alam
PKI	*Public-Key Infrastructure*
PKS	Polisi Keselamatan Siber
SMS	*Short Message Service*
UPS	*Uninterruptible Power Supply*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

TAFSIRAN

4IR	Revolusi Industri Keempat (4IR) - Transformasi disruptif dalam industri melalui penggunaan teknologi baru muncul. Ia bercirikan teknologi baharu yang menggabungkan alam fizikal, digital dan biologi yang memberi kesan kepada semua bidang, industri dan ekonomi
Antivirus	Perisian yang digunakan untuk mengesan dan membuang *malware*, seperti virus komputer, *adware, backdoors, malicious BHO's, dialers, fraudtools, hijackers, keyloggers, malicious LSPs, rootkits, spyware, trojan horses dan worms.*
Ancaman	Penyebab bagi insiden-insiden tidak diingini yang boleh mengakibatkan kemudaratan kepada sistem dan organisasi serta berupaya mengancam keselamatan negara
Ancaman siber	Ancaman yang berpunca daripada Internet atau rangkaian menggunakan laluan komunikasi data yang memberi kesan terhadap kerahsiaan, integriti dan ketersediaan sistem maklumat dari dalam agensi mahupun dari jarak jauh serta penyebaran maklumat melalui medium siber yang bertentangan dengan undang-undang negara serta berupaya menggugat keselamatan negara
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang di bawah tanggungjawab Kementerian/ Jabatan/ Agensi.
Aset alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
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.
BCM/ PKP	*Business Continuity Management*/ Pelan Kesinambungan Perkhidmatan
CCTV	*Close-circuit television system*. Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
CSIRT	*Computer Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan Siber yang ditubuhkan untuk membantu Kementerian/ Jabatan/ Agensi mengurus pengendalian insiden keselamatan siber.

CDO	*Chief Digital Officer* - Ketua Pegawai Digital yang bertanggungjawab terhadap tadbir urus pendigitalan bagi menyokong arah tuju Jabatan.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Enkripsi	Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Enterprise Architecture (EA)	Rangka kerja strategik bagi mengenal pasti dan memperkemas semula perkhidmatan yang disediakan dengan memahami struktur, fungsi, perkhidmatan, proses kerja, data yang digunakan serta aplikasi dan teknologi yang menyokong perkhidmatan organisasi.
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.
Harta Intelek	Apa-apa karya, ciptaan, rekaan, variasi baru tumbuhan, maklumat sulit termasuk rahsia perdagangan yang layak untuk mendapat perlindungan di bawah mana-mana undang-undang harta intelek, khususnya undang-undang hak cipta, paten, reka bentuk perindustrian, cap dagangan, petunjuk geografi, reka bentuk susun atur litar bersepadu, jenis baru tumbuhan dan undang-undang '*Common Law*'
Hotfix	Kemas kini perisian yang direka untuk menangani isu atau kelemahan tertentu dalam program atau sistem dengan cepat, tanpa menunggu pelancaran (*release*) yang dijadualkan.
ICTSO	*ICT Security Officer* - Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer
Insiden Keselamatan Siber	Kejadian siber yang tidak diingini apabila berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan pelanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber

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 Terhad	Kawasan terhad ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang dibenarkan sahaja dan aktiviti yang dilakukan di tempat tersebut seperti seperti di Pusat Data dan Bilik Fail.
Kriptografi	Kaedah untuk menukar data dan maklumat biasa kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat.
Libraries	Koleksi kod, fungsi, atau rutin yang telah ditulis sebelum ini yang boleh digunakan oleh pengaturcara untuk melaksanakan tugas tertentu tanpa perlu menulis kod tersebut dari awal.
Load balancing	Teknik yang digunakan untuk mengagihkan trafik rangkaian atau beban aplikasi ke pelbagai pelayan, sumber, atau sambungan untuk mengoptimumkan penggunaan sumber, meminimumkan masa respons, dan memastikan kebolehpercayaan sistem.
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 Storan	Bermaksud peralatan mudah alih yang boleh menyimpan maklumat atau data. Contoh: *external hard disk*, CD/DVD, *backup tape* dan lain-lain.
Mobile code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi- fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
Outsource	Menggunakan perkhidmatan luar atau melaksanakan fungsifungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

Pair programming	Pembangunan perisian secara kolaborasi. Melibatkan dua pembangun sistem yang berkerjasama mengunakan satu komputer. Proses pemerhatian dan semakan kod aturcara dibuat secara bersama.
Patches	Kemas kini atau pembetulan yang diterapkan pada program perisian atau sistem operasi untuk menangani kelemahan, meningkatkan fungsionaliti, atau memperbaiki prestasi.
Pegawai Keselamatan	Termasuk pegawai yang dilantik sebagai Pegawai Keselamatan Kerajaan atau mana-mana pegawai yang berkhidmat sebagai Pegawai Keselamatan Kerajaan atau pegawai yang menjalankan tugas sebagai Pegawai Keselamatan Kerajaan
Perisikan Ancaman	Perisikan ancaman merujuk kepada usaha mengumpul, menganalisis, dan menggunakan maklumat mengenai ancaman yang boleh membahayakan keselamatan negara. Ini termasuk ancaman dari dalam dan luar negara seperti pengganas, pengintip, dan kegiatan subversif.
Pemilik Projek	Pemilik Projek adalah pihak yang bertanggungjawab ke atas keseluruhan proses bisnes di dalam projek
Pemilik Sistem	Pemilik sistem (*business owner*) bagi sistem yang dibangunkan atau yang paling banyak memiliki data.
Pengurus ICT	Pegawai yang mengetuai Bahagian Teknologi Maklumat di Jabatan.
Pentadbir Pusat Data	Pentadbir yang mengurus dan menyelenggara Pusat Data Jabatan.
Pentadbir Rangkaian ICT	Pentadbir yang melaksana dan menyelenggara rangkaian dan keselamatan.
Pentadbir Sistem Aplikasi	Pentadbir yang menyelenggarakan sistem aplikasi, laman web dan aplikasi mudah alih serta mengurus operasi/ sokongan teknikal.
Pentadbir Aset	Pentadbir yang bertanggungjawab terhadap penggunaan dan pengurusan sesebuah aset ICT
Pentadbir Sistem	Merujuk kepada semua pentadbir bagi pusat data, rangkaian dan keselamatan, laman web, pangkalan data, sistem aplikasi, e-mel dan aset ICT

Pembekal	Individu, syarikat atau kumpulan syarikat yang dilantik untuk memperbaharui, membekal, menghantar, memasang, mentauliah, membangunkan, menguji, dan menyelenggara perkakasan atau perisian di Jabatan.
Pengguna	Merujuk kepada kakitangan jabatan dan pihak ketiga yang dibenarkan untuk menggunakan sesuatu sumber ICT di Jabatan.
Pihak Ketiga	Pihak Ketiga terdiri daripada pembekal, pakar runding dan pihakpihak lain yang berkepentingan dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT Jabatan atau pelawat yang mengunjungi Jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan Jabatan melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Refactoring	Menambaik kod sumber sedia ada dengan mengekalkan fungsi kod tersebut
Source code	Kod sumber atau kod program yang ditulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
Technical Service Design	Proses merancang dan mencipta aspek teknikal sesuatu perkhidmatan untuk memastikan ia memenuhi keperluan pengguna dan bisnes.
Test-driven development	Kaedah pembangunan sistem yang mempunyai aktiviti pengujian secara terus. Setiap kod dan fungsi sistem yang dibangunkan dalam fasa pembangunan akan terus diuji fungsinya tanpa menunggu sistem siap sepenuhnya. lanya bertujuan mengurangkan ralat dan meningkatkan tahap keselamatan.
Threat intelligence	Pengumpulan, analisis, dan penyebaran maklumat mengenai potensi atau ancaman sedia ada kepada keselamatan organisasi
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan.
Web Content Filtering	Teknologi yang digunakan untuk mengawal dan menyekat akses kepada laman web atau kandungan dalam talian tertentu berdasarkan kriteria yang telah ditetapkan.

PERKARA 1.0: PENGENALAN

Polisi Keselamatan Siber Institut Tanah dan Ukur Negara (PKS INSTUN) mengandungi amalan baik yang mesti dibaca dan dipatuhi semasa menggunakan aset Teknologi Maklumat dan Komunikasi atau *Information Technology and Communication* (ICT). Polisi ini juga menerangkan kepada pengguna mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT jabatan.

1.1 OBJEKTIF

PKS INSTUN diwujudkan untuk menjamin kesinambungan urusan jabatan dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi jabatan. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi dengan baik.

Objektif utama PKS INSTUN ini diwujudkan adalah seperti berikut:

a) Memastikan kelancaran operasi jabatan dan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, ketersediaan, kesahihan maklumat dan komunikasi; dan
c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

1.2 PERNYATAAN POLISI

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
b) Menjamin setiap maklumat adalah tepat dan sempurna;
c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

a) **KERAHSIAAN** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) **INTEGRITI** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c) **TIDAK BOLEH DISANGKAL** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
d) **KESAHIHAN** - Data dan maklumat hendaklah dijamin kesahihannya; dan
e) **KETERSEDIAAN** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

PERKARA 2: SKOP

Skop PKS INSTUN meliputi perkara berikut:

a) **Maklumat**: Pangkalan data dan fail data, kontrak dan perjanjian, sistem dokumentasi, maklumat penyelidikan, manual pengguna, bahan latihan, prosedur operasi dan sokongan, pelan kesinambungan perkhidmatan, *fallback arrangements*, jejak audit (*audit trails*) dan maklumat arkib;

b) **Platform Aplikasi dan Perisian**: Perisian aplikasi, perisian sistem, alat pembangunan (*development tools*) dan utiliti (*utilities*);

c) **Peranti Fizikal dan Sistem**: Peralatan komputer, peralatan komunikasi, media mudah alih dan lain-lain peralatan;

d) **Aliran Data**: Merujuk kepada aliran transaksi data menggunakan saluran komunikasi yang dikenal pasti, direkodkan dan dikaji semula secara berkala seperti e-mel rasmi;

e) **Sistem Luaran**: Sistem bukan milik jabatan yang dihubungkan dengan sistem Jabatan;

f) **Sumber Luaran**: Perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Jabatan seperti perkhidmatan pengkomputeran dan komunikasi, utiliti umum seperti pencahayaan, elektrik dan pendingin hawa;

g) **Manusia**: Kelayakan, kemahiran dan pengalaman; dan

h) **Aset tidak nyata (*intangibles*)**: Seperti reputasi dan imej organisasi.

Semua warga jabatan adalah bertanggungjawab memastikan dan memulihara maklumat dan data berdasarkan perkara berikut:

a) Maklumat dan data hendaklah boleh dicapai secara berterusan dengan cepat, tepat, mudah dan dengan cara yang diyakini selamat bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

b) Semua maklumat dan data hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta melindungi kepentingan jabatan, perkhidmatan dan masyarakat.

c) Mengenal pasti semua maklumat dan data yang dijana atau di kumpul dan diasingkan mengikut kategori maklumat seperti Maklumat Rahsia Rasmi, Maklumat Rasmi, Maklumat Pengenalan Diri dan Data Terbuka.

d) Bagi memastikan keselamatan maklumat yang berterusan, PKS merangkumi perlindungan semua bentuk maklumat dan data kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan. Ini dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan/ prosedur dalam pengendalian maklumat dan aset.

PERKARA 3.0: PRINSIP KESELAMATAN

Prinsip PKS INSTUN ini adalah seperti berikut:

a) **Prinsip Perlu Tahu**

Capaian dibenarkan dan dihadkan kepada pengguna tertentu atas dasar "perlu tahu" berdasarkan klasifikasi maklumat dan tahap tapisan keselamatan pengguna.

b) **Hak Keistimewaan Minimum**

Hak capaian kepada pengguna dimulai pada tahap yang paling minimum. Kelulusan adalah perlu bagi membolehkan capaian pada tahap yang lebih tinggi.

c) **Kawalan Capaian Berdasarkan Peranan**

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

d) **Peminimuman Data**

Mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

e) **Akauntabiliti**

Setiap pengguna adalah bertanggung jawab ke atas semua tindakan terhadap kemudahan ICT jabatan yang disediakan. Tanggungjawab pengguna termasuk perkara berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya sentiasa tepat dan lengkap;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan maklumat; dan
v. Mematuhi langkah dan garis panduan keselamatan yang ditetapkan.

f) **Pengasingan Tugas**

Setiap tugasan, proses dan persekitaran pelaksanaan ICT hendaklah dipisahkan dan diasingkan sebaik mungkin untuk mengekalkan integriti dan perlindungan keselamatan daripada kesilapan dan penyalahgunaan. Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:

i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;
ii. Persekitaran penerimaan iaitu peringkat di mana sesuatu aplikasi diuji; dan
iii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

g) **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden atau keadaan yang mengancam keselamatan. Pengauditan adalah penting dalam menjamin akauntabiliti seperti berikut:

i. Mengesan pematuhan atau perlanggaran polisi keselamatan;
ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran polisi keselamatan; dan
iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran polisi keselamatan.

h) **Pematuhan**

Prinsip ini penting untuk mengelak perlanggaran polisi melalui tindakan berikut:

i. Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;
ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;
iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan
iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

i) **Pemulihan**

Pemulihan adalah untuk memastikan ketersediaan dan kebolehcapaian dengan meminimumkan gangguan atau kerugian akibat daripadanya adalah seperti berikut:

i. Merancang dan menguji Pelan Pemulihan Bencana (DRP); dan
ii. Melaksanakan amalan terbaik dalam pelaksanaan ICT.

j) **Saling Bergantung**

Prinsip keselamatan adalah saling lengkap melengkapi dan hendaklah dipatuhi bagi jaminan keselamatan yang berkesan. Tindakan mempelbagaikan pendekatan dalam menyusun strategi mekanisme keselamatan mampu meningkatkan tahap keselamatan.

PERKARA 4.0: PENILAIAN RISIKO KESELAMATAN MAKLUMAT

INSTUN hendaklah mengambil kira kewujudan risiko ke atas Aset ICT akibat dari ancaman dan kerentanan yang semakin meningkat hari ini. Justeru itu INSTUN perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko Aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas Aset ICT.

INSTUN hendaklah melaksanakan proses penilaian risiko keselamatan maklumat secara berkala (sekurang-kurangnya sekali dalam setahun) sama ada secara dalaman (*in-house*) atau melalui perkhidmatan pihak ketiga yang bertauliah dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat termasuklah aplikasi, perisian, pelayan, rangkaian dan/ atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan kemudahan pemprosesan maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam. Mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) menerima dan/ atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c) mengelak dan/ atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/ atau mencegah berlakunya risiko; dan
d) memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 5.0 – KAWALAN ORGANISASI

KAWALAN 5.1 - POLISI KESELAMATAN MAKLUMAT	
Objektif: Memastikan hala tuju pengurusan perlindungan maklumat adalah selaras dengan keperluan perkhidmatan jabatan dan peraturan serta undang-undang.	
5.1.1 Pelaksanaan Polisi Keselamatan Siber INSTUN	**Tanggungjawab**
PKS INSTUN ini dilaksanakan oleh KJ dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada CDO, ICTSO dan lain-lain pegawai yang dilantik.	i. KJ ii. JPICT
5.1.2 Pemakaian Polisi	**Tanggungjawab**
PKS INSTUN ini terpakai kepada semua kakitangan INSTUN dan juga pihak ketiga yang berurusan dengan INSTUN.	Semua kakitangan INSTUN dan juga pihak ketiga
5.1.3 Penyelenggaraan Polisi	**Tanggungjawab**
PKS INSTUN ini tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Setiap perubahan hendaklah mendapat pengesahan ICTSO. Perubahan yang melibatkan penambahan atau pemansuhan yang memberi impak ke atas keselamatan adalah dianggap perubahan utama dan hendaklah mendapat pengesahan JPICT INSTUN. Prosedur semakan semula polisi ini adalah seperti berikut: a) Menyemak sekurang-kurangnya satu (1) kali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan pindaan atau perubahan secara bertulis; dan c) Memaklumkan pindaan atau perubahan polisi yang telah dipersetujui kepada semua pengguna.	ICTSO

KAWALAN 5.2 – TANGGUNGJAWAB DAN PERANAN KESELAMATAN MAKLUMAT	
Objektif: Menerangkan peranan dan tanggungjawab struktur tadbir urus individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber	
5.2.1 Peranan dan tanggungjawab KJ	**Tanggungjawab**
Peranan dan tanggungjawab KJ adalah seperti berikut: a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber jabatan; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan siber INSTUN; c) Merancang, menyelaras dan menyeragamkan pelaksanaan program/ projek-projek keselamatan siber jabatan supaya selaras dengan Pelan Strategik Pendigitalan INSTUN; d) Memastikan keperluan sumber bagi keselamatan siber INSTUN adalah mencukupi; dan e) Memastikan pelaksanaan penilaian risiko keselamatan siber INSTUN. f) Memastikan semua pengguna mematuhi PKS INSTUN; g) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); h) Melantik CDO dan ICTSO serta memaklumkan pelantikan kepada pihak yang bertanggungjawab; i) Menguatkuasa dan meluluskan PKS INSTUN; dan j) Mengambil maklum terhadap aduan pelanggaran PKS INSTUN.	KJ

5.2.2 Peranan dan tanggungjawab Ketua Pegawai Digital (CDO)	Tanggungjawab
KJ bertanggungjawab melantik CDO di jabatan. Peranan dan tanggungjawab CDO adalah seperti berikut: a) Membantu KJ dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber; b) Menentukan keperluan dan bertanggungjawab ke atas perkara-perkara berkaitan dengan keselamatan siber INSTUN; c) Membangun dan menyelaras pelaksanaan program kesedaran dan latihan keselamatan siber. d) Meneraju inisiatif pendigitalan di INSTUN melalui penggunaan data, analitis dan teknologi digital, e) Mewujudkan budaya berpacukan data dalam sektor awam yang mengamalkan pendekatan *principle-based* melalui penggunaan data dan teknologi digital; dan f) Mentransformasi penyampaian perkhidmatan digital di INSTUN berfokuskan pengalaman pelanggan (*customer experience*) yang berteraskan konsep *Whole of-Government* (WoG) melalui inovasi melibatkan perkongsian data, data terbuka dan teknologi baru muncul; g) Menilai, menyelaras, memperaku keperluan perkhidmatan digital, *Technical Service Design* dan bajet pembangunan serta mengurus agensi sebagai pelaksana inisiatif dan projek pendigitalan; h) Meneraju perubahan melalui Penjajaran Pelan Strategik Pendigitalan (PSP) INSTUN dengan: i) Memastikan PSP INSTUN selari dengan PSP Sektor Awam dan Pengurusan Risiko dan Pelan Pengurusan Perubahan; j) Memantapkan struktur tadbir urus pendigitalan jabatan & menyelaras penggunaan dasar, standard dan amalan terbaik global.	CDO

5.2.3 Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO)	Tanggungjawab
a) Memastikan semua infrastruktur keselamatan ICT INSTUN menepati prinsip-prinsip keselamatan berpandukan Rangka Dasar Keselamatan ICT dan Arahan Keselamatan Kerajaan serta Polisi Keselamatan Siber (PKS) INSTUN; b) Menyedia dan mengkaji semula dokumen infrastruktur keselamatan ICT INSTUN bagi tujuan audit keselamatan ICT; c) Mengenal pasti bidang-bidang keselamatan ICT INSTUN yang perlu diberikan perhatian rapi; d) Memastikan tahap keselamatan ICT di INSTUN adalah terjamin setiap masa; e) Memastikan semua kakitangan INSTUN memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah Rangka Dasar Keselamatan ICT Kerajaan dan Polisi Keselamatan Siber (PKS) INSTUN; f) Menjalankan penilaian risiko dan program-program keselamatan ICT di INSTUN; g) Mewujudkan pelan tindakan bagi mengurus risiko akibat daripada ketidakpatuhan kepada standard, garis panduan dan prosedur keselamatan ICT INSTUN; h) Melaporkan kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara (MKN) mengenai sebarang insiden keselamatan ICT yang berlaku di INSTUN; i) Membantu dalam membangunkan standard, garis panduan dan prosedur untuk aplikasi, sistem dan infrastruktur ICT di INSTUN bagi mematuhi Dasar Keselamatan ICT Kerajaan;	ICTSO

j) Mewujudkan program-program bagi meningkatkan pengetahuan, kesedaran dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber dan peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT di INSTUN; k) Menyebar dan menyalurkan amaran awal terhadap ancaman-ancaman yang berpotensi menyebabkan kerosakan besar kepada aset ICT jabatan; dan l) Mengurus keseluruhan program-program keselamatan ICT di INSTUN.	
5.2.4 Peranan dan tanggungjawab Pengurus ICT	**Tanggungjawab**
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan INSTUN; b) Melaporkan ancaman atau insiden keselamatan siber kepada ICTSO; c) Menentukan kawalan capaian pengguna terhadap aset ICT; d) Memastikan penyimpanan rekod, bahan bukti dan laporan ancaman atau insiden keselamatan siber INSTUN dilaksanakan dengan berkesan; e) Memastikan semua pengguna diberi penerangan dan pembudayaan serta mematuhi peruntukan di bawah PKS INSTUN serta memperakukan Akuan Pematuhan PKS seperti di **Lampiran A(I)**; f) Menetapkan hala tuju pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; g) Memantau had capaian pengguna;	Pengurus ICT

h) Memantau punca ancaman atau insiden keselamatan ICT dan memastikan tindakan membaik pulih dilaksanakan dengan segera; i) Berperanan sebagai Koordinator *Disaster Recovery Plan* (DRP) untuk mengaktifkan Pelan Pemulihan Bencana ICT INSTUN; j) Menguatkuasakan dan memantau pelaksanaan PKS INSTUN; dan k) Mengenal pasti tindakan ke atas pelanggaran PKS dan memaklumkan dalam JPICT.	
5.2.5 Jawatankuasa Pemandu ICT (JPICT)	**Tanggungjawab**
Peranan dan tanggungjawab Jawatankuasa Pemandu ICT (JPICT) adalah sebagai struktur organisasi formal yang diwujudkan untuk mengurus dan mematuhi keselamatan siber jabatan seperti berikut: a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT jabatan; b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju / strategi ICT jabatan c) Merancang dan menyelaras pembangunan program / projek ICT jabatan supaya selaras dengan pelan strategik organisasi dan pelan strategik ICT; d) Menyelaras dan menyeragamkan pembangunan dan pelaksanaan ICT di jabatan dengan pelan strategik organisasi dan pelan strategik ICT Sektor Awam; e) Mempromosi dan menggalakkan perkongsian pintar projek ICT antara jabatan; f) Merancang dan menentukan langkah-langkah keselamatan ICT;	JPICT

g) Mengikuti dan memantau perkembangan program ICT INSTUN serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pembangunan dan pelaksanaan ICT; h) Menilai dan meluluskan semua perolehan ICT INSTUN berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; i) Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi INSTUN kepada JTISA untuk kelulusan teknikal; j) Mengemukakan laporan projek ICT yang diluluskan di peringkat JPICT INSTUN dan dibuat perolehan kepada JTISA; dan k) Mengemukakan laporan kemajuan projek ICT bagi INSTUN yang telah diluluskan oleh JPICT/ JTISA kepada JTISA mengikut tempoh yang telah ditetapkan.	

KAWALAN 5.3 – PENGASINGAN TUGAS

Objektif: Menerangkan perbezaan tugas setiap individu dengan lebih jelas dan teratur untuk mencegah daripada berlakunya kebocoran serta kesilapan maklumat serta mematuhi dan melaksanakan prinsip-prinsip PKS.

5.3.1 Pentadbir Rangkaian dan Keselamatan	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut: a) memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) beroperasi sepanjang masa; b) memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c) merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d) mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;	Pentadbir Rangkaian Dan Keselamatan

e) melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT; f) memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian jabatan secara tidak sah seperti melalui peralatan modem dan *dial-up*; g) Menganalisis log trafik rangkaian dan menyekat aktiviti yang tidak normal. h) menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; i) memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; j) Membantu penyediaan Pelan Pemulihan Bencana (DRP); dan k) Membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP).	
5.3.2 Pentadbir Laman Web	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Laman Web INSTUN adalah seperti berikut: a) menerima kandungan Laman Web INSTUN yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b) memantau prestasi capaian dan menjalankan ujian penalaan (*tuning*) prestasi untuk memastikan akses yang lancar; c) memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka Laman Web INSTUN; d) mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet;	Pentadbir Laman Web INSTUN

e) memastikan hanya maklumat yang bersifat terbuka dipaparkan di Laman Web INSTUN; f) memastikan reka bentuk Laman Web INSTUN dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; g) melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*; h) memantau proses *backup* dan *restoration* ke atas kandungan Laman Web INSTUN dan sistem aplikasi; dan i) melaporkan sebarang pelanggaran keselamatan Laman Web INSTUN kepada ICTSO.	
5.3.3 Pentadbir Pangkalan Data	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a) melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b) memastikan pangkalan data beroperasi sepanjang masa dan berada dalam keadaan selamat; c) melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data; d) memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; e) melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip PKS; f) membantu penyediaan Pelan Pemulihan Bencana (DRP); g) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP); h) melaksanakan proses perkemasan data (*housekeeping*) di dalam pangkalan data;	Pentadbir Pangkalan Data

i) menganalisis log capaian pangkalan data dan menyekat aktiviti yang tidak normal; dan j) melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.	
5.3.4 Pentadbir Pusat Data	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut: a) memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat; b) memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data; c) menjadualkan dan melaksanakan proses sandaran dan pemulihan ke atas pangkalan data dan sistem secara berkala; d) membantu penyediaan Pelan Pemulihan Bencana (DRP); e) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP); f) memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan; g) melaporkan sebarang pelanggaran keselamatan Pusat Data INSTUN kepada ICTSO; dan h) menyediakan laporan semakan pusat data secara berkala; dan i) melaksanakan proses replikasi sistem aplikasi kritikal ke Pusat Pemulihan Bencana (DRC).	Pentadbir Pusat Data
5.3.5 Pentadbir Sistem Aplikasi	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a) memastikan persekitaran sistem aplikasi berada dalam keadaan selamat; b) membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;	

c) memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; d) membantu penyediaan Pelan Pemulihan Bencana (DRP); e) membantu pelaksanaan simulasi Pelan Pemulihan Bencana (DRP); f) memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; g) menyimpan dan menganalisis rekod jejak audit; h) memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemas kini supaya terhindar daripada ancaman virus dan penggodam; i) mengenal pasti aktiviti yang tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran; j) membatalkan atau memberhentikan aktiviti yang tidak normal dengan serta merta; dan k) melaporkan kepada ICTSO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.	Pentadbir Sistem Aplikasi
5.3.6 Pentadbir E-mel	**Tanggungjawab**
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: a) menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b) pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c) mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi.	Pentadbir E-mel

5.3.7 Pegawai Aset ICT	Tanggungjawab
Pegawai Aset ICT ialah pegawai yang dilantik oleh Pegawai Pengawal. Peranan dan tanggungjawab Pegawai Aset ICT adalah seperti berikut: a) memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; b) memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik oleh Ketua Jabatan/ Bahagian; c) memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan sistem pengurusan aset Kerajaan yang berkuat kuasa dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; d) memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan secara bertulis daripada Ketua Jabatan/ Pegawai Aset/ Pegawai-pegawai lain yang diberi kuasa oleh Ketua Jabatan; e) memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ naik-taraf aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira; f) memastikan pelaksanaan pemeriksaan, pelupusan dan hapus kira Aset ICT dilaksanakan mengikut keperluan; g) memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama Jabatan/ Bahagian berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan; h) memastikan setiap kerosakan Aset ICT Kerajaan dilaporkan; i) memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;	Pegawai Aset ICT

j) memastikan senarai daftar induk aset ICT Kerajaan disediakan; k) memastikan senarai aset ICT disediakan dan dipaparkan di lokasi; l) memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan; dan m) bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan Merekodkan kan penyelenggaraan aset ICT Kerajaan; n) memastikan setiap kes kehilangan Aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur	
5.3.8 Pengguna	**Tanggungjawab**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a) membaca, memahami, dan mematuhi PKS INSTUN; b) menjaga kerahsiaan kata laluan yang diberikan; c) menjaga kerahsiaan maklumat INSTUN yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan,penyimpanan,penghantaran,penyampaian, d) pertukaran dan pemusnahan; e) mengetahui dan memahami implikasi keselamatan ICT akibat daripada tindakannya; f) menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan); g) melaporkan sebarang aktiviti atau insiden keselamatan ICT kepada ICTSO dengan segera; h) menghadiri program-program kesedaran mengenai keselamatan ICT; dan i) menandatangani Akuan Pematuhan Polisi Keselamatan Siber Jabatan (Lampiran A), Borang Akta Rahsia Rasmi 1972 (Lampiran B atau yang setara dengannya) dan mengisi Borang Tapisan Keselamatan.	Pengguna

5.3.9 Pihak Ketiga	Tanggungjawab
Terdiri daripada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dalam penggunaan atau capaian kepada aset dan perkhidmatan ICT INSTUN atau pelawat yang mengunjungi INSTUN. Peranan dan tanggungjawab adalah seperti berikut: a) membaca, memahami, dan mematuhi PKS INSTUN; b) menjaga kerahsiaan kata laluan yang diberikan; c) menjaga kerahsiaan maklumat jabatan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; d) mengetahui dan memahami implikasi keselamatan ICT akibat daripada tindakannya; e) menjaga kerahsiaan maklumat walaupun perjanjian atau pelantikan telah tamat; f) Pergerakan hendaklah diiringi oleh pegawai bertanggungjawab INSTUN; dan g) mengisi Akuan Pematuhan Polisi Keselamatan Jabatan, Borang Akta Rahsia Rasmi (Lampiran B(I) dan Lampiran B (II)), dan mengisi Borang Tapisan Keselamatan.	Pihak Ketiga
KAWALAN 5.4 – TANGGUNGJAWAB PENGURUSAN	
Objektif: Memastikan pihak pengurusan dan Kakitangan INSTUN memahami peranan serta memenuhi tanggungjawab dalam keselamatan maklumat.	
a) Pengurusan hendaklah memastikan kakitangan INSTUN yang mempunyai urusan dengan perkhidmatan ICT INSTUN supaya mengamalkan keselamatan menurut polisi dan prosedur yang telah ditetapkan. b) CDO dan ICTSO hendaklah memastikan semua Kakitangan INSTUN serta pihak ketiga diberi taklimat berkaitan pematuhan ke atas PKS INSTUN;	CDO/ ICTSO

c) memastikan Kakitangan INSTUN serta pihak ketiga bertanggungjawab ke atas keselamatan Aset ICT berdasarkan peraturan yang ditetapkan oleh INSTUN; dan d) memastikan sumber yang mencukupi untuk melaksanakan proses dan kawalan yang berkaitan keselamatan ICT.	

KAWALAN 5.5 – HUBUNGAN DENGAN PIHAK BERKUASA

Objektif: Menyediakan senarai perhubungan pihak berkuasa berkaitan sekiranya berlaku kejadian yang menjejaskan keselamatan maklumat dan perkhidmatan ICT.

5.5.1 Hubungan Dengan Pihak Berkuasa Keselamatan Dan Pihak Utiliti	**Tanggungjawab**
Hubungan yang baik dengan pihak berkuasa seperti berikut tidak terhad kepada hendaklah dikekalkan: a) Malaysian Emergency Response System 999 (Polis, Bomba, Agensi Pertahanan Awam Malaysia); b) National Disaster Management Agency (NADMA); c) National Cyber Security Agency (NACSA); d) Suruhanjaya Komunikasi dan Multimedia (SKMM) e) CyberSecurity Malaysia; f) Pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan; dan g) Pihak Berkuasa Tempatan (PBT). Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab INSTUN; b) Mewujud dan mengemas kini prosedur/ senarai pihak berkuasa perundangan/ pihak yang dihubungi semasa kecemasan; dan	ICTSO

c) Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	
KAWALAN 5.6 – HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN KHAS	
Objektif: Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan INSTUN disediakan.	
5.6.1 Hubungan Dengan Kumpulan Pakar Keselamatan dan Pertubuhan Profesional	**Tanggungjawab**
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional ataupun forum bagi: a) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	ICTSO
KAWALAN 5.7 – PERISIKAN ANCAMAN	
Objektif: Memastikan kawalan ancaman keselamatan terhadap INSTUN difahami, di analisa dan mengambil tindakan yang bersesuaian.	
5.7.1 Pengumpulan Maklumat Ancaman	**Tanggungjawab**
Maklumat yang berkaitan dengan ancaman keselamatan maklumat hendaklah di kumpul berdasarkan perkara-perkara berikut:	ICTSO/ CSIRT

a) Mengenal pasti ancaman keselamatan yang boleh menyebabkan gangguan kepada INSTUN melalui: i. Ancaman yang telah berlaku sebelum ini. ii. Ancaman yang mungkin berlaku sekiranya tiada tindakan pencegahan proaktif diambil. iii. Ancaman yang mungkin berlaku walaupun pencegahan proaktif telah diambil. iv. Ancaman juga boleh dikenal pasti melalui penyemakan dokumen, log serta aduan pelanggan; dan pertanyaan kepada pemilik atau pengguna aset, kakitangan organisasi serta pakar pengurusan keselamatan maklumat dalam dan luar organisasi. b) Mengenal pasti jenis ancaman seperti di bawah: i. Secara strategik: Kategori penyerang atau serangan; ii. Secara taktikal: Metodologi, kaedah, alatan dan teknologi yang digunakan; iii. Secara operasi: Butiran khusus tentang serangan. iii. Mengumpul maklumat daripada sumber dalaman dan luaran yang terpilih.	
5.7.2 Analisa Maklumat Ancaman	**Tanggungjawab**
Maklumat ancaman yang dikumpulkan hendaklah dianalisa bagi memahami tujuan ancaman, sumber maklumat dan kaitan dengan INSTUN	i. ICTSO ii.Pentadbir Rangkaian ICT
5.7.3 Tindakan Ke Atas Maklumat Ancaman	**Tanggungjawab**
Maklumat ancaman yang telah di analisa hendaklah diambil tindakan berdasarkan perkara berikut: a) Menyediakan peralatan atau perisian yang mengawal ancaman keselamatan; b) Melaksanakan proses penilaian risiko ke atas ancaman keselamatan maklumat;	i.ICTSO ii.Pentadbir Rangkaian ICT

c) Penambahbaikan kawalan keselamatan dengan peningkatan fungsi bagi peralatan seperti *firewall, intrusion detection system* (IDS) atau anti perisian hasad; dan d) Sebagai kegunaan untuk pengujian keselamatan maklumat.	

KAWALAN 5.8 – KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK	
Objektif: Memastikan keselamatan maklumat diambil kira dalam pengurusan projek.	
5.8.1 Pengurusan Projek	**Tanggungjawab**
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh Pihak Ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Risiko keselamatan maklumat hendaklah dinilai dan diambil kira di peringkat awal bagi sesuatu projek; b) Keperluan keselamatan maklumat perlu ditangani pada peringkat awal pelaksanaan projek; c) Mengambil kira risiko dalaman dan luaran keselamatan maklumat semasa pelaksanaan projek; d) Semakan dan keberkesanan pelaksanaan penguraian risiko keselamatan maklumat hendaklah diuji dan dinilai.	i. Pengurus ICT/Ketua Seksyen ii. ICTSO iii. Pengurus Projek iv. Pasukan Projek
5.8.2 Keselamatan Maklumat Dalam Pengurusan Projek	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti maklumat yang terlibat selari dengan keperluan keselamatan INSTUN dan berpotensi memberikan impak negatif; b) Perlindungan perlu mengambil kira kerahsiaan, integriti dan ketersediaan; c) Memastikan jaminan keselamatan maklumat berkaitan identiti pihak ketiga dilaksanakan dan disahkan; d) Memastikan kawalan akses kepada pihak ketiga;	i. Pengurus ICT/ Ketua Seksyen ii. ICTSO iii. Pengurus Projek/ Pasukan Projek

e) Memaklumkan kepada pengguna tentang tugas dan tanggungjawab mereka; f) Melaksanakan pemantauan ke atas log transaksi dan kebocoran maklumat oleh pihak ketiga; g) Pematuhan kepada undang-undang dan peraturan yang berkuat kuasa; h) Memastikan klausa keselamatan maklumat yang berkaitan diambil kira di dalam perjanjian atau kontrak; i) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; j) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; k) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem maklumat hendaklah mengambil kira kawalan keselamatan; l) Sistem maklumat yang dibangunkan sama ada secara dalaman atau luaran hendaklah dikaji supaya mengikut keperluan pengguna dan selaras dengan dasar atau peraturan berkaitan yang berkuat kuasa; m) Sistem maklumat yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; dan n) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan.	
KAWALAN 5.9 – INVENTORI MAKLUMAT DAN ASET	
Objektif: Memastikan setiap aset hendaklah dikenal pasti, di kelas, di rekod dan di selenggara untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT.	

5.9.1 Inventori dan Pemilikan Aset ICT	Tanggungjawab
Semua aset ICT di INSTUN mestilah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) Setiap aset ICT hendaklah didaftarkan dan ditentukan pemiliknya. Ketua Jabatan atau Ketua Bahagian adalah bertanggungjawab mengenal pasti pemilik aset ICT tersebut; b) Pemilik aset hendaklah menentukan tahap sensitiviti (terperingkat) yang bersesuaian bagi setiap maklumat aset di jabatan. Pemilik aset juga hendaklah membuat keputusan dalam menentukan individu yang dibenarkan untuk capaian dan penggunaan maklumat tersebut; c) Pentadbir aset ICT adalah bertanggungjawab untuk menentukan prosedur kawalan khas (contohnya: kawalan capaian), kaedah pelaksanaan dan penyelenggaraan serta menyediakan langkah pemulihan yang konsisten dengan arahan pemilik aset; d) Semua pengguna aset ICT mestilah mematuhi keperluan kawalan yang telah ditetapkan oleh pemilik aset atau pentadbir sistem. Pengguna adalah terdiri daripada kakitangan jabatan (lantikan tetap, pinjaman, kontrak dan sambilan), konsultan, kontraktor atau pihak ketiga yang terlibat secara langsung; e) Kehilangan/ kecurian aset ICT mestilah dilaporkan serta merta mengikut prosedur pengurusan kehilangan/ kecurian aset berpandukan Arahan Perbendaharaan yang telah ditetapkan; f) Senarai maklumat aset di INSTUN hendaklah diwujudkan. Setiap aset perlu ditentukan dengan jelas dan pemilikan aset mestilah dipersetujui dan didokumenkan berserta lokasi semasa aset tersebut. Senarai aset hendaklah disimpan oleh ketua jabatan atau ketua bahagian; dan	i. Ketua Jabatan ii. Pegawai Aset ICT yang dilantik iii. Pengguna

g) Setiap pengguna adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan aset ICT di bawah tanggungannya.	
5.9.2 Inventori Maklumat Dan Aset	**Tanggungjawab**
Semua maklumat dan Aset ICT di INSTUN hendaklah diuruskan mengikut peraturan dan tatacara yang berkuat kuasa seperti berikut: a) Memastikan maklumat dan Aset ICT yang dikenal pasti direkodkan serta dikemas kini mengikut Tatacara Pengurusan Aset Alih Kerajaan; b) Memastikan pengemaskinian maklumat berkaitan instalasi dan perubahan aset; c) Maklumat pemilik Aset ICT, lokasi dan status Aset ICT hendaklah dikemas kini dari semasa ke semasa; d) Setiap maklumat dan Aset ICT perlu diklasifikasikan mengikut kategori kerahsiaan; e) Memastikan Aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja. Penukaran pemilik hendaklah dilaksanakan sekiranya terdapat perubahan; dan f) Pemeriksaan Aset ICT hendaklah dilaksanakan sekurang-kurangnya satu (1) kali setahun. Rujuk tatacara pengurusan aset alih kerajaan.	Pegawai Aset ICT yang dilantik
5.9.2 Tanggungjawab Pemilik	**Tanggungjawab**
Pemilik aset ICT perlu bertanggungjawab berkaitan pengurusan aset seperti perkara berikut: a) Memastikan semua aset ICT di bawah kawalan pemilik hendaklah didaftarkan, diklasifikasikan, dilindungi dan disemak secara berkala, terkini dan tepat; b) Memastikan semua aset yang mempunyai kebergantungan disenaraikan;	Pengguna

c) Keperluan untuk penggunaan maklumat dan aset yang diterima ditetapkan; d) Memastikan kawalan akses dilaksanakan mengikut kategori kerahsiaan dan disemak secara berkala; e) Kehilangan/kecurian Aset ICT mestilah dilaporkan serta merta mengikut tatacara Pengurusan Aset Alih Kerajaan; f) Semua maklumat dan aset ICT yang dimusnahkan dan dilupuskan hendaklah dikendalikan mengikut garis panduan sanitasi media elektronik yang berkuat kuasa dan Tatacara Pengurusan Aset Alih Kerajaan; dan g) Bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan Aset ICT di bawah kawalannya.	
KAWALAN 5.10 – PENGGUNAAN MAKLUMAT DAN ASET	
Objektif : Memastikan setiap maklumat dan Aset ICT yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.	
5.10.1 Penggunaan Maklumat dan Aset	**Tanggungjawab**
Langkah-langkah yang perlu diambil termasuklah seperti berikut: a) Pengguna dan pihak ketiga yang mempunyai capaian ke atas maklumat dan Aset ICT hendaklah bertanggungjawab terhadap keperluan perlindungan serta pengendalian keselamatan maklumat; b) Menyediakan prosedur pengurusan pengendalian maklumat yang merangkumi penggunaan, kebenaran, perkongsian dan pemantauan maklumat; c) Memastikan kawalan capaian yang dibenarkan mengikut tahap klasifikasi pengelasan maklumat; d) Menyelenggara rekod berkaitan senarai pengguna yang dibenarkan untuk capaian maklumat;	Semua

e) Memastikan kawalan ke atas salinan maklumat, storan maklumat dan perlu melaksanakan pelabelan media storan dengan jelas; dan f) Memperoleh kebenaran untuk melaksanakan pelupusan maklumat dan aset berdasarkan kaedah yang bersesuaian.	
5.10.2 Peminjaman Aset	**Tanggungjawab**
Langkah-langkah yang perlu diambil termasuklah seperti berikut: a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh INSTUN bagi membawa keluar peralatan bagi tujuan yang dibenarkan; b) Melindungi dan mengawal peralatan sepanjang masa; c) Merekodkan kan aktiviti peminjaman dan pemulangan peralatan; dan d) Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.	Pengguna
KAWALAN 5.11 – PEMULANGAN ASET	
Objektif: Memastikan proses pemulangan aset ICT dilaksanakan apabila berlaku perubahan dan penamatan perkhidmatan, kontrak atau perjanjian.	
5.11.1 Pemulangan Aset ICT	**Tanggungjawab**
a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan atau terma perkhidmatan yang ditetapkan bagi pegawai yang: i. Bertukar keluar; ii. Bersara; iii. Cuti melebihi tiga (3) bulan iv. Ditamatkan perkhidmatan; dan v. Diarahkan oleh Ketua Jabatan.	i. Kakitangan Jabatan ii. Pegawai Aset yang dilantik

b) Bagi aset persendirian yang digunakan bagi tujuan rasmi hendaklah dimaklumkan dan dikawal mengikut prosedur yang ditetapkan; c) Memastikan semua aset ICT dikembalikan oleh pihak ketiga setelah tamat kontrak mengikut terma yang ditetapkan; d) Semua aset ICT yang dipulangkan tidak terhad kepada perkara berikut: i. Peranti pengguna; ii. Media storan luaran/ mudah alih; iii. Peralatan khas; dan iv. Peralatan pengesahan identiti seperti token dan *smart card*. v. Salinan fizikal maklumat.	
KAWALAN 5.12 – PENGELASAN MAKLUMAT	
Objektif: Memastikan pengenalpastian dan pemahaman tentang keperluan perlindungan maklumat mengikut kepentingan di INSTUN.	
5.12.1 Pengelasan Maklumat	**Tanggungjawab**
Pengelasan maklumat bertujuan memastikan setiap maklumat diberi perlindungan oleh pemilik aset untuk menentukan keperluan, keutamaan dan tahap keselamatan berdasarkan peraturan yang berkuat kuasa seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; d) Terhad; dan Data Terbuka.	Pegawai Pengelas yang dilantik
KAWALAN 5.13 – PELABELAN MAKLUMAT	
Objektif : Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.	
5.13.1 Pelabelan dan Pengendalian Maklumat	**Tanggungjawab**

Semua maklumat mestilah dilabelkan mengikut klasifikasi maklumat seperti yang dinyatakan pada para 5.12.1 Pengelasan Maklumat. a) Aktiviti yang melibatkan pemprosesan maklumat seperti penyalinan, penyimpanan, penghantaran (sama ada dari segi lisan, pos, faksimile dan mel elektronik) dan pemusnahan maklumat mestilah mengikut standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; dan b) Maklumat yang diklasifikasikan sebagai Rahsia Besar, Rahsia, Sulit dan Terhad perlu dilindungi daripada didedahkan kepada pihak ketiga atau awam. Pihak ketiga jika perlu boleh diberi kebenaran capaian maklumat INSTUN atas dasar perlu tahu sahaja dan mestilah mendapat kebenaran daripada INSTUN. c) Contoh kaedah pelabelan termasuk: a. label fizikal; b. *header dan footer;* c. *metadata;* d. *watermark*; dan d) *rubber stamps.*	Pengguna
5.13.2 Pengendalian Media Penyimpanan Maklumat	**Tanggungjawab**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan tidak berlaku pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah dan yang boleh mengganggu aktiviti perkhidmatan; b) Prosedur perlu disediakan untuk pengurusan peralatan penyimpanan maklumat mudah alih;	i. Ketua Jabatan/ Pentadbir Aset ii. Pengguna iii. Pihak Ketiga

c) Peralatan penyimpanan maklumat yang tidak digunakan perlu dilupuskan secara selamat mengikut prosedur yang telah ditetapkan; d) Prosedur untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada didedah tanpa kebenaran atau disalah guna; e) Dokumentasi sistem perlu dilindungi daripada capaian yang tidak dibenarkan; f) Polisi, prosedur dan kawalan pertukaran maklumat yang rasmi perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi dalam agensi dan mana-mana pihak terjamin; g) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara agensi dengan pihak luar; h) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari agensi; i) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya; dan j) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat agensi.	
KAWALAN 5.14 – PEMINDAHAN MAKLUMAT	
Objektif : Memastikan keselamatan maklumat terjamin semasa pertukaran maklumat dengan entiti luar.	
5.14.1 Prosedur Pemindahan Maklumat	**Tanggungjawab**
Perkara yang perlu diambil kira bagi semua pemindahan maklumat adalah seperti berikut: a) Kawalan ke atas pemindahan maklumat daripada diceroboh, diubah, disalin, dimusnahkan dan sebagainya;	i. ICTSO/ Pengguna/ Pentadbir Sistem

b) Pemindahan maklumat hendaklah direkod bagi kawalan pengesanan; c) Memastikan kakitangan yang dibenarkan sahaja bertanggungjawab semasa pemindahan maklumat; d) Mengenal pasti pegawai yang bertanggungjawab sekiranya berlaku insiden keselamatan; e) Memastikan kawalan keselamatan dilaksanakan berdasarkan peringkat pengelasan maklumat; f) Ketersediaan dan boleh dipercayai bagi perkhidmatan pemindahan maklumat yang digunakan; g) Mematuhi peraturan dan pekeliling semasa yang masih berkuat kuasa berkaitan pemusnahan maklumat; h) Pematuhan kepada mana-mana undang-undang/peraturan/pekeliling yang berkaitan dengan pemindahan data; i) Mengehadkan pemindahan maklumat untuk tujuan rasmi dan yang dibenarkan sahaja; dan j) Menandatangani *Non-Disclosure Agreements* (NDA) bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat seperti di **Lampiran B (I) dan Lampiran B (II).**	ii. Pihak Ketiga
5.14.2 Pemindahan Elektronik	**Tanggungjawab**
Perkara berikut hendaklah diambil kira bagi pemindahan secara elektronik: a) Memastikan kawalan keselamatan untuk mengesan perisian hasad; b) Melindungi lampiran bagi dokumen rahsia rasmi; c) Mencegah penghantaran mesej atau dokumen kepada alamat e-mel yang salah; d) Mendapatkan kelulusan untuk menggunakan perkhidmatan luar seperti storan awan, perkongsian fail dan media sosial;	i. CDO ii. Pengurus ICT iii. ICTSO iv. Pentadbir Rangkaian ICT v. Pihak ketiga

e) Menggunakan pengesahan yang selamat sekiranya pemindahan maklumat menggunakan rangkaian awam melalui *Virtual Private Network*; f) Memastikan kawalan sekatan ke atas fungsi *forwarding* ke alamat e-mel persendirian; g) Memastikan penggunaan SMS dan aplikasi media sosial tidak menghantar maklumat rahsia rasmi; dan h) Memastikan Maklumat elektronik yang hendak dipindahkan perlu dilindungi menggunakan enkripsi *Secure Socket Layer (SSL)* dan *Application Programming Interface (API).* i) Sebarang penggunaan tandatangan elektronik hendaklah merujuk kepada peraturan/ pekeliling semasa yang berkuat kuasa atau merujuk kepada klausa 8.24 – Penggunaan Kriptografi	
5.14.3 Pemindahan Storan Fizikal	**Tanggungjawab**
Perkara yang perlu dipatuhi semasa pemindahan storan fizikal adalah seperti berikut: a) Bertanggungjawab mengawal dan memberikan makluman semasa penghantaran atau penerimaan; b) Memastikan alamat penghantaran yang betul; c) Pembungkusan storan fizikal perlu dilindungi daripada kerosakan semasa pemindahan; d) Senarai kurier yang boleh dipercayai dan dipersetujui oleh pihak Pengurusan; e) Memastikan semasa penghantaran fizikal tidak berlaku pengubahsuaian tanpa kebenaran; f) Menyimpan log rekod terakhir kandungan media storan, maklumat penerima dan masa ke lokasi pemindahan; dan g) Memastikan semua pemindahan pita fizikal direkod menggunakan borang Pengurusan Tape Backup.	i.Pengurus ICT ii. ICTSO iii. Pentadbir Pusat Data

5.14.4 Pemindahan Lisan	Tanggungjawab
Perkara yang perlu diambil kira bagi pemindahan lisan adalah seperti berikut: a) Tidak membincangkan maklumat rahsia rasmi secara lisan dalam komunikasi yang tidak selamat; b) Tidak meninggalkan maklumat rahsia rasmi dalam peti rakaman suara; c) Memastikan bilik yang sesuai disediakan seperti bilik kedap bunyi; dan d) Perbincangan maklumat terperingkat perlu dimaklumkan kepada kakitangan yang terlibat.	Pengurus ICT

KAWALAN 5.15 – KAWALAN CAPAIAN

Objektif : Memastikan akses maklumat dan aset diberikan kepada pihak yang dibenarkan.

5.15.1 Keperluan Kawalan Capaian	Tanggungjawab
Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menentukan jenis akses bagi individu atau kumpulan yang diperlukan ke atas maklumat dan lain-lain yang berkaitan aset; b) Aspek keselamatan aplikasi; c) Akses kawalan kemasukan fizikal yang sesuai; d) Kebenaran dan penyebaran maklumat bergantung kepada tahap keselamatan serta klasifikasi maklumat; e) Mengawal had akses istimewa; f) Pengasingan tugas dan fungsi kawalan akses seperti kebenaran akses mengikut tahap capaian; g) Permohonan akses secara rasmi; h) Pengurusan hak akses; dan	i. ICTSO ii. Pengurus ICT iii. Pentadbir Sistem Aplikasi

i) Rekod log	
5.15.2 Prinsip Kawalan Akses	**Tanggungjawab**
Prinsip kawalan akses yang harus dipertimbangkan semasa hak akses diberikan adalah: a) **"Perlu tahu"** – Entiti hanya diberikan akses ke atas maklumat yang diperlukan untuk melaksanakan tugasnya seperti had akses yang berbeza mengikut peranan; b) **"Perlu guna"** – Entiti yang memerlukan akses kepada infrastruktur maklumat; c) Hak akses dibenarkan kepada semua kecuali perkara yang melanggar peraturan; d) Menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang; dan e) Melaksanakan semakan ke atas hak akses yang diberikan	i. Pengurus ICT ii. Pentadbir Sistem Aplikasi
KAWALAN 5.16 – PENGURUSAN IDENTITI	
Objektif : Memastikan ID pengguna adalah unik dan sesuai ke atas entiti untuk mengakses sistem dan aset lain yang berkaitan.	
5.16.1 Pengurusan Capaian Pengguna	**Tanggungjawab**
Proses pengurusan identiti perlu memastikan perkara berikut dipatuhi: a) Memastikan ID pengguna hendaklah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; b) Memastikan identiti yang diberikan kepada lebih dari seorang individu (identiti bersama) hanya dibenarkan jika ada keperluan dan tertakluk kepada kelulusan serta direkodkan; c) Memastikan perkakasan yang memerlukan ID pengguna hendaklah mendapatkan kelulusan serta pengawasan berterusan;	i. ICTSO ii. Pengurus ICT iii. Pentadbir Sistem Aplikasi iv. Pengguna v. Pihak Ketiga

d) Memastikan pendaftaran ID pengguna didaftarkan untuk setiap pengguna adalah unik; e) Merekodkan kan semua penggunaan dan pengurusan identiti pengguna; f) Sebarang pembatalan ID pengguna hendaklah berdasarkan pada arahan dari bahagian berkaitan. g) Membatal, menamatkan, menukar peranan atau menyahaktif akaun pengguna atas sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Cuti melebihi 3 bulan; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
5.16.2 Prosedur Penyediaan Atau Pembatalan Akses	**Tanggungjawab**
Prosedur bagi penyediaan atau pembatalan akses perlu memastikan perkara berikut: a) Memastikan identiti yang diwujudkan memenuhi keperluan tugasan berkaitan; b) Mengesahkan identiti pengguna yang memohon sebelum pengwujudan ID pengguna; c) Mewujudkan ID pengguna; d) Mengkonfigurasi dan mengaktifkan ID pengguna; dan e) Menyediakan atau membatalkan hak akses berdasarkan kelulusan atau pemakluman.	i. Pengurus ICT ii. Pentadbir Sistem Aplikasi
KAWALAN 5.17 – PENGESAHAN MAKLUMAT	
Objektif : Memastikan pengesahan entiti yang betul untuk mengelakkan kegagalan capaian maklumat.	
5.17.1 Kawalan Capaian Sistem dan Aplikasi	**Tanggungjawab**
Kawalan capaian sistem dan aplikasi perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan.	Pentadbir ICT/ Pengguna

a) Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: i. Menyediakan kaedah yang sesuai atau terkini untuk pengesahan capaian (*authentication*); dan ii. Mengehadkan tempoh penggunaan mengikut kesesuaian. b) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Menamatkan sesuatu sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan; dan ii. Mengehadkan tempoh sambungan ke sesuatu aplikasi berisiko tinggi. iii. Mengawal fungsi *multi-session* bagi aplikasi kritikal atau mengikut keperluan c) Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara berikut hendaklah dipatuhi: i. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; ii. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); iv. Mengehadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; v. Pengguna digalakkan membuat enkripsi dengan menukarkan teks biasa (*plain text*) kepada bentuk *ciphertext* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. vi. Penjanaan kata laluan peribadi sementara semasa proses pendaftaran yang unik untuk	

setiap individu. Pengguna diwajibkan menukar kata laluan apabila log masuk kali pertama; vii. Menghantar kata laluan kepada pengguna dengan cara yang selamat; viii. Kata laluan *default* bagi pihak ketiga perlu ditukar serta-merta selepas selesai pemasangan sistem, perkakasan atau perisian; dan ix. Menguruskan kata laluan menggunakan kaedah penyimpanan rekod yang diluluskan dan selamat.	
5.17.2 Pengurusan Kata Laluan	**Tanggungjawab**
Sistem pengurusan kata laluan perlu: a) Memastikan penggunaan ID pengguna dan kata laluan tidak dikongsi; b) Membenarkan pengguna menukar kata laluan sendiri; c) Menguatkuasakan kata laluan yang kukuh mengikut cadangan amalan baik; d) Mewajibkan pengguna menukar kata laluan apabila log masuk kali pertama; e) Tidak memaparkan kata laluan di skrin ketika log masuk; f) Mengelakkan penggunaan kata laluan yang berulang; dan g) Menggalakkan pengguna menukar kata laluan sekurang kurangnya setiap enam (6) bulan untuk ke semua sistem utama.	Pentadbir ICT/ Pengguna
5.17.3 Pengurusan Kata Laluan Super Administrator	**Tanggungjawab**
Pentadbir ICT bagi pengurusan kata laluan Super Administrator perlu: a) Memastikan penggunaan ID pengguna dan kata laluan tidak dikongsi; b) Memastikan pilihan kata laluan yang berkualiti. Merujuk klausa 5.17.4 (g);	Pentadbir ICT/ Ketua Jabatan

c) Menyimpan kata laluan di dalam sampul surat yang *sealed* di dalam peti besi/ kabinet berkunci; dan d) Menukar kata laluan sekurang-kurangnya setiap 12 bulan untuk semua sistem utama.	
5.17.4 Tanggungjawab Pengguna	**Tanggungjawab**
Pengguna perlu mematuhi amalan terbaik penggunaan kata laluan seperti berikut: a) Pengguna tidak seharusnya menulis atau menyimpan kata laluan tanpa enkripsi di atas talian melainkan pada kes-kes tertentu di mana ia diperlukan oleh prosedur operasi seperti penyimpanan *root ID* dan kata laluan bagi sistem utama. Di dalam hal ini, kata laluan haruslah dilindungi dengan menggunakan mekanisme kawalan lain seperti menyimpan kata laluan di dalam laci berkunci dan menggunakan kata laluan yang berbeza bagi capaian berbeza; b) Pengguna adalah tidak digalakkan mengguna kata laluan yang sama bagi kegunaan sistem di jabatan mahupun sistem yang tidak terdapat di jabatan; c) Pengguna hendaklah tidak mendedahkan kata laluan yang diguna pakai di jabatan kepada sesiapa. Ini termasuklah ahli keluarga dan bukan ahli keluarga apabila melakukan kerja pejabat di rumah. Walau bagaimanapun, bagi ID kata laluan utama yang disimpan di dalam laci berkunci, harus diadakan satu proses mengenai tatacara memperoleh kata laluan berkenaan sekiranya berlaku ketidakhadiran pemegang kata laluan utama sewaktu ia diperlukan; d) Pengguna haruslah menyimpan kata laluan dengan selamat dan tidak dibenarkan berkongsi akaun dengan pengguna lain. Pengguna yang disahkan adalah bertanggungjawab ke atas kerahsiaan dan keselamatan kata laluan dan akaun mereka;	Pengguna

e) Penggunaan atribut *remember me* adalah tidak dibenarkan sama sekali. Sekiranya akaun atau kata laluan disyaki telah dicerobohi, maka laporan kejadian hendaklah dilaporkan kepada pasukan *Cyber Security Incident Response Team* (CSIRT) INSTUN/ dan tindakan menukar kata laluan perlu dilakukan; f) Menggunakan kata laluan yang sukar diramal. Kata laluan adalah bukan perkataan di dalam mana-mana bahasa, dialek, loghat dan sebagainya. Kata laluan tidak seharusnya berdasarkan maklumat peribadi, nama ahli keluarga dan seumpamanya; dan g) Sistem pengurusan kata laluan hendaklah menekankan pilihan kata laluan yang berkualiti. Kata laluan yang berkualiti antara lainnya mempunyai ciri-ciri seperti berikut: i. Gabungan kombinasi antara huruf, nombor dan simbol (seperti: 0-9, a-z, A-Z, ! @ # $ % ^ & * ( ) - +) selari dengan amalan terbaik terkini; dan ii. Kata laluan yang ditentukan oleh pengguna hendaklah tidak digunakan semula. Pengguna haruslah tidak membina kata laluan yang sama atau seakan-akan serupa seperti mana yang pernah digunakan sebelum ini di tempat lain. Khususnya, lima (5) kata laluan yang pernah digunakan sebelum ini tidak digunakan semula.	
KAWALAN 5.18 – HAK CAPAIAN	
Objektif : Memastikan hak capaian kepada maklumat dan aset lain dibenarkan mengikut keperluan.	
5.18.1 Pendaftaran Dan Pembatalan Hak Capaian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk mencapai maklumat dan perkhidmatan;	i.Pentadbir Rangkaian/ Pentadbir Sistem ii.Pengguna

b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; d) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pengemaskinian dan atau pembatalan hendaklah diambil atas sebab bertukar, berpindah, bersara dan atau tamat perkhidmatan. e) Aktiviti capaian oleh pengguna direkod dan diselenggarakan dengan sistematik dari semasa ke semasa. Maklumat yang di rekod termasuk identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya; dan f) Akaun pengguna yang baru diwujudkan perlu diberikan kata laluan sementara dan pengguna perlu menukar kata laluan apabila log masuk dibuat pada kali pertama.	
KAWALAN 5.19 – KESELAMATAN MAKLUMAT DENGAN HUBUNGAN PEMBEKAL	
Objektif : Memastikan aset dilindungi sepenuhnya daripada akses yang tidak sewajarnya oleh pembekal.	
5.19.1 Polisi Keselamatan Maklumat ke atas Pembekal	**Tanggungjawab**
Semua pembekal adalah tertakluk kepada garis panduan/peraturan mengenai keselamatan yang berkuat kuasa. Perkara- perkara yang perlu dipatuhi adalah seperti berikut: a) Pembekal hendaklah menandatangani Surat Akuan Pematuhan PKS jabatan; b) Pembekal hendaklah menandatangani Akuan Akta	ICTSO/ Pembekal

Rahsia Rasmi 1972; c) Pembekal hendaklah menjalani ujian tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); dan d) Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas.	
KAWALAN 5.20 – MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PEMBEKAL	
Objektif: Memastikan keselamatan maklumat dengan pihak ketiga melalui perjanjian yang telah dipersetujui.	
5.20.1 Kawalan Keselamatan Maklumat Melalui Perjanjian dengan Pembekal	**Tanggungjawab**
Perjanjian dengan pihak pembekal hendaklah merangkumi keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan perkhidmatan teknologi maklumat dan komunikasi.	CDO, Pengurus ICT dan Pembekal
5.20.2 Kawalan Keselamatan Maklumat Dengan Pembekal dan Pihak Ketiga	**Tanggungjawab**
Perjanjian dengan pembekal hendaklah meliputi risiko keselamatan yang merangkumi perkhidmatan ICT dan kesinambungan bekalan produk dengan pihak ketiga.	ICTSO, Pengurus ICT, Pembekal
KAWALAN 5.21 – PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI DAN KOMUNIKASI (ICT)	
Objektif: Memastikan persetujuan kawalan keselamatan bersama pihak ketiga dimeterai.	
5.21.1 Kawalan Rantaian Bekalan Maklumat Dan Komunikasi	**Tanggungjawab**
Perjanjian dengan pihak ketiga hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. Perkara yang perlu diambil kira adalah seperti berikut:	i. Pengurus ICT ii. Pengurus Projek iii. Pihak Ketiga

a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pihak ketiga hendaklah menghebahkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c) Mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan; d) Memastikan jaminan dari pihak ketiga bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; e) Memastikan komponen produk yang dibekalkan adalah tulen dan tidak diubah dari spesifikasi asal atau mengikut keperluan; f) Memastikan bahawa produk ICT memenuhi standard keselamatan yang ditetapkan atau melalui proses pensijilan rasmi atau amalan terbaik; g) Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara Jabatan dan pihak ketiga; dan h) Memastikan pengurusan kitaran hayat dan ketersediaan komponen ICT yang tidak lagi tersedia disebabkan pihak ketiga tidak lagi beroperasi atau pihak ketiga tidak lagi menyediakan komponen ini disebabkan kemajuan teknologi. Ini bagi mengurangkan impak risiko keselamatan ke atas jabatan.	

KAWALAN 5.22 – PEMANTAUAN, SEMAKAN DAN UBAHSUAI PENGURUSAN PERKHIDMATAN PEMBEKAL	
Objektif: Memastikan tahap keselamatan maklumat dan pembekalan perkhidmatan selaras dengan perjanjian pembekal.	
5.22.1 Pemantauan dan Penilaian Perkhidmatan Pembekal	**Tanggungjawab**
a) Jabatan hendaklah memantau dan menyemak perkhidmatan pembekal secara berkala.	Pengurus Projek

b) Melaksanakan tindakan susulan terhadap sebarang ketidakpatuhan perkhidmatan yang diberikan oleh pembekal berdasarkan kepada perjanjian yang berkuat kuasa	
5.22.2 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut SOP yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Perubahan di dalam perjanjian bersama pembekal; b) Perubahan yang dilakukan oleh jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian, teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengurus ICT
KAWALAN 5.23 – KESELAMATAN MAKLUMAT UNTUK KEGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN	
Objektif: Memastikan pengurusan keselamatan maklumat bagi pengkomputeran awan.	
5.23.1 Keselamatan Maklumat Menggunakan Perkhidmatan Awan	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti klasifikasi maklumat atau data dalam penggunaan perkhidmatan pengkomputeran awan; b) Mengenal pasti ciri-ciri asas dan model perkhidmatan pengkomputeran awan yang hendak digunakan; c) Menetapkan tugas dan tanggungjawab ke atas pengurusan perkhidmatan awan;	i. Pengurus ICT ii. ICTSO iii. Pentadbir Pusat Data iv. Pihak ketiga

d) Menentukan tanggungjawab kawalan keselamatan perkhidmatan awan di antara penyedia dan pengguna perkhidmatan awan; e) Memastikan kemampuan dan jaminan kawalan keselamatan maklumat yang dilaksanakan oleh penyedia perkhidmatan awan; f) Struktur tadbir urus hendaklah dikenal pasti berdasarkan peranan dan tanggungjawab untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat dalam pengurusan pengkomputeran awan; Pematuhan pengurusan maklumat rahsia rasmi dalam persekitaran ICT menjadi prasyarat (*prerequisite*) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan; h) Memastikan pengurusan kontrak dan terma keselamatan dalam penggunaan perkhidmatan pengkomputeran awan; i) Memastikan perlindungan migrasi data ke pengkomputeran awan, perlindungan data semasa penghantaran dan perlindungan data dalam simpanan logikal atau fizikal oleh pihak penyedia perkhidmatan; j) Memantau, menyemak dan menilai keselamatan maklumat dalam perkhidmatan pengkomputeran awan; k) Memastikan pengurusan insiden oleh penyedia perkhidmatan pengkomputeran awan; l) Memastikan penyedia perkhidmatan mewujudkan atau mempunyai pelan pengurusan kesinambungan perkhidmatan (PKP); dan m) Memastikan penamatan perkhidmatan pengkomputeran awan dilaksanakan mengikut peraturan berkuat kuasa.	

KAWALAN 5.24 – PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Memastikan perancangan pengurusan insiden keselamatan maklumat yang dilaksanakan adalah konsisten dan teratur.	
5.24.1 Tanggungjawab Dan Prosedur	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Mewujudkan prosedur bagi mengendalikan pengurusan insiden keselamatan maklumat; b) Memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat; c) Pemakluman kepada agensi kerajaan pusat yang bertanggungjawab atau Agensi Keselamatan Siber Negara (NACSA) dalam menangani insiden keselamatan; dan d) Menyediakan latihan yang bersesuaian kepada pasukan teknikal yang bertanggungjawab ke atas insiden keselamatan.	i. ICTSO/ Pengurus ICT ii. Ketua Pasukan CSIRT
5.24.2 Pelantikan Pegawai Bertanggungjawab	**Tanggungjawab**
Perkara yang perlu diambil kira seperti berikut: a) Penilaian risiko ke atas insiden yang berlaku; b) Pemantauan, pengkelasan, analisis dan laporan insiden perlu disediakan sama ada secara manual atau melalui sistem;	i. Ketua Pasukan CSIRT ii. Pengurus ICT iii. ICTSO
KAWALAN 5.25 – PENILAIAN INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Mengenal pasti kategori dan penilaian berasaskan keutamaan ke atas semua insiden keselamatan maklumat.	
5.25.1 Penilaian dan Keputusan Insiden Keselamatan Maklumat	**Tanggungjawab**
Jabatan hendaklah menilai sama ada serangan diklasifikasikan sebagai insiden. **Menentukan Keutamaan Tindakan Ke Atas Insiden**	Pasukan CSIRT

Tindakan ke atas insiden yang dilaporkan akan dibuat berasaskan tahap kritikal sesuatu insiden. Keutamaan akan ditentukan seperti berikut: a) **Keutamaan 1:** Insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan Negara, kestabilan ekonomi, imej, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. b) **Keutamaan 2:** Insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1.	
KAWALAN 5.26 – TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT	
Objektif: Melaksanakan tindak balas yang cepat dan berkesan terhadap insiden keselamatan maklumat.	
5.26.1 Pelaporan Insiden Keselamatan Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Sekiranya berstatus Keutamaan 1, jabatan hendaklah melaporkan insiden kepada agensi kerajaan pusat yang bertanggungjawab bagi tujuan penyelarasan dan memaklumkan kepada agensi yang menyelianya dalam tempoh 24 jam selepas insiden dikesan serta mengaktifkan Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan, BCP*) dan Pelan Pemulihan Bencana (*Disaster Recovery Plan, DRP*) sekiranya perlu. b) Bagi Keutamaan 2, jabatan hendaklah melaksanakan pengendalian insiden secara kendiri dan seterusnya memaklumkan kepada agensi kerajaan pusat yang bertanggungjawab dan agensi yang menyelianya setelah proses pengendalian insiden dan pemulihan pada peringkat agensi selesai.	Pasukan CSIRT

c) Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada Pasukan CSIRT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; d) Mematuhi prosedur operasi standard (SOP) keselamatan ICT jabatan; e) Menyimpan jejak audit dan memelihara bahan bukti; dan f) Menyediakan dan melaksanakan pelan tindakan pemulihan.	

KAWALAN 5.27 – PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT	
Objektif : Meningkatkan kawalan keselamatan berdasarkan analisa dan penyelesaian insiden keselamatan maklumat yang telah dilaksanakan bagi mengelakkan insiden yang sama berulang.	
5.27.1 Pengajaran Dari Insiden Keselamatan Maklumat	**Tanggungjawab**
Penilaian insiden yang perlu diambil kira adalah seperti berikut: a) Menambah baik pelan pengurusan insiden; b) Mengenal pasti punca insiden yang kerap berlaku bagi melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan risiko; dan c) Meningkatkan kesedaran keselamatan maklumat kepada kakitangan INSTUN.	i. CDO ii.ICTSO iii.Pasukan CSIRT

KAWALAN 5.28 – PENGUMPULAN BUKTI	
Objektif: Memastikan pengurusan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undang-undang.	
5.28.1 Pengumpulan dan Pengendalian Bukti	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut:	i. ICTSO/ Pengurus ICT ii. Pasukan CSIRT

a) Mengenal pasti, mengumpul, menyimpan dan melindungi bahan bukti untuk mengelakkan pengubahsuaian tanpa kebenaran; b) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti bahan bukti; dan c) Sistem maklumat perlu merekodkan kan semua bukti insiden selaras dengan tarikh dan masa kejadian.	

KAWALAN 5.29 – KESELAMATAN MAKLUMAT SEMASA GANGGUAN

Objektif: Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

5.29.1 Melindungi Maklumat dan Aset semasa gangguan	**Tanggungjawab**
Jabatan harus melaksanakan: a) Kawalan keselamatan maklumat, sistem sokongan dan aset dalam Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana (DRP); b) Proses untuk mengekalkan kawalan keselamatan maklumat yang sedia ada semasa gangguan; c) Kawalan sementara atau kaedah manual bagi meneruskan kesinambungan perkhidmatan ICT.	i. CDO ii. Pasukan PKP iii. Pasukan DRP

KAWALAN 5.30 - KESEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN

Objektif : Menjamin operasi perkhidmatan dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

5.30.1 Pelan Pemulihan Bencana (DRP)	**Tanggungjawab**
Menyediakan Pelan Pemulihan Bencana untuk mengekalkan kesinambungan perkhidmatan ICT. Pelan ini mestilah diperakui oleh pihak pengurusan jabatan dan perkara-perkara berikut perlu diberi perhatian: a) Melantik ahli Pasukan Pemulihan Bencana; b) Mengenal pasti dan mendokumenkan semua tanggungjawab dan prosedur kecemasan atau pemulihan;	i. ICTSO ii. Pasukan DRP

c) Mengenal pasti *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) untuk sistem aplikasi kritikal mengikut keutamaan; d) Melaksanakan pengujian dan simulasi pemulihan bencana sekurang – kurangnya sekali setahun bagi memastikan pemulihan dapat dilakukan dalam jangka masa yang telah ditetapkan seperti yang tertakluk dalam pelan pemulihan bencana; e) Mengadakan program kesedaran dan latihan kepada pengguna mengenai prosedur kecemasan;	
KAWALAN 5.31 - KEPERLUAN UNDANG-UNDANG, BERKANUN, PERATURAN DAN KONTRAK	
Objektif: Bagi memastikan pematuhan kepada keperluan undang-undang yang berkaitan dengan keselamatan maklumat. Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan perlu ditakrifkan, didokumenkan, disimpan dan dikemas kini.	
5.31.1 Pematuhan Polisi	**Tanggungjawab**
Adalah menjadi tanggungjawab Ketua Jabatan untuk memastikan bahawa pematuhan dan sebarang perlanggaran dielakkan. Langkah-langkah perlu bagi mengelakkan sebarang pelanggaran perundangan termasuklah memastikan setiap pengguna membaca, memahami dan mematuhi Polisi Keselamatan Siber INSTUN dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.	Semua
5.31.2 Keperluan Perundangan	**Tanggungjawab**
Kakitangan Jabatan perlu memastikan senarai perundangan dan peraturan yang berkuat kuasa dari semasa ke semasa perlu dipatuhi oleh semua kakitangan di jabatan	Semua

5.31.3 Pelanggaran Perundangan	Tanggungjawab
Mengambil tindakan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan termasuk Polisi Keselamatan Siber yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972. Antara tindakan yang boleh diambil terhadap pihak ketiga adalah penamatan kontrak.	Semua
5.31.4 Kawalan Kriptografi	**Tanggungjawab**
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi kriptografi; b) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah direka untuk mempunyai fungsi kriptografi; c) Sekatan ke atas penggunaan enkripsi; dan d) Kaedah akses oleh pihak berkuasa Malaysia mengenai maklumat enkripsi perkakasan dan perisian.	i. Entiti Berkaitan ii. Pihak Ketiga
KAWALAN 5.32 – HAK HARTA INTELEK	
Objektif: Bagi memastikan pematuhan ke atas undang-undang terhadap harta intelek.	
5.32.1 Pematuhan Terhadap Hak Harta Intelek (*Intellectual Property Rights*)	**Tanggungjawab**
Prosedur pengawalan hendaklah dilaksanakan bagi memastikan pematuhan kepada perundangan, peraturan dan keperluan kontrak berkaitan produk yang mempunyai IPR termasuk perisian *proprietary*.	i. Semua ii. Pihak ketiga
KAWALAN 5.33 – PERLINDUNGAN REKOD	
Objektif: Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan rekod.	

5.33.1 Keselamatan Dokumen	Tanggungjawab
Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a) Mematuhi Panduan Pengurusan Rekod Sektor Awam yang berkuat kuasa b) Memastikan sistem dokumentasi atau penyimpanan dokumen adalah selamat dan kehilangan atau kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; c) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; d) Pergerakan fail terperingkat dan dokumen rahsia rasmi hendaklah mengikut prosedur keselamatan; e) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; f) Dokumen terperingkat rasmi perlu dienkripsikan sebelum dihantar secara elektronik; dan g) Memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak.	Semua
KAWALAN 5.34 - PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI	
Objektif: Bagi memastikan pematuhan ke atas undang-undang yang berkaitan dengan aspek Keselamatan maklumat peribadi.	
5.34.1 Perlindungan dan Privasi Data Peribadi	**Tanggungjawab**
a) Kakitangan perlu sedar bahawa data kegunaan peribadi yang dijana dalam aset ICT adalah milik jabatan. b) Pihak pengurusan tidak menjamin kerahsiaan data peribadi yang disimpan dalam aset ICT. c) Untuk tujuan keselamatan dan penyelenggaraan rangkaian, pegawai yang diberi kuasa perlu mengawasi peralatan, sistem dan rangkaian.	Semua

d) Pihak pengurusan berhak mengaudit rangkaian dan sistem secara berkala bagi memastikan ia mematuhi PKS. e) Pihak pengurusan perlu menggalakkan dasar privasi yang adil dan bertanggungjawab bagi memastikan semua maklumat peribadi digunakan berdasarkan keperluan untuk mengelakkan penyalahgunaan maklumat. f) Pendedahan maklumat peribadi tentang kakitangan jabatan kepada pihak ketiga tidak sepatutnya berlaku kecuali: i. dikehendaki oleh undang-undang atau peraturan; ii. dengan persetujuan yang jelas dan nyata daripada kakitangan tersebut; atau iii. setelah menerima persetujuan bertulis daripada pihak ketiga di mana maklumat akan dilindungi dengan tahap keselamatan dan privasi yang mencukupi seperti yang ditentukan oleh unit undang-undang serta perjanjian jelas diperoleh daripada pengurusan sumber manusia; dan iv. rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrak dan keperluan jabatan.	
KAWALAN 5.35 - KAJIAN BEBAS KESELAMATAN MAKLUMAT	
Objektif: Bagi memastikan pendekatan yang digunakan bersesuaian, cukup dan berkesan secara lebih efektif.	
5.35.1 Semakan Keselamatan Maklumat	**Tanggungjawab**
Semakan keselamatan maklumat mestilah diambil kira seperti berikut: a) Pematuhan pemeriksaan ke atas PKS, piawaian dan prosedur perlu dilakukan secara tahunan. Pemeriksaan ini mestilah melibatkan usaha bagi menentukan kawalan yang mencukupi dan dipatuhi;	ICTSO/ Pengurus ICT

b) Agensi yang terlibat dengan ISMS akan menjalani proses pengauditan (pensijilan, pemantauan pertama, pemantauan kedua). Bagi agensi yang tidak melaksanakan ISMS, perlu ditentukan kawalan yang bersesuaian seperti pemeriksaan/ semakan berkala; dan c) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.	

KAWALAN 5.36 - PEMATUHAN KEPADA POLISI, PERATURAN DAN PIAWAIAN UNTUK KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dilaksanakan mengikut polisi keselamatan maklumat serta piawaian dan peraturan semasa.	
5.36.1 Akuan Pematuhan Polisi Keselamatan Siber	**Tanggungjawab**
Ketua Jabatan adalah bertanggungjawab untuk memastikan setiap pegawai menandatangani **Akuan Pematuhan Polisi Keselamatan Siber** seperti di **LAMPIRAN A(I).**	i.Ketua Jabatan ii. ICTSO

KAWALAN 5.37 – DOKUMENTASI PROSEDUR OPERASI	
Objektif: Prosedur operasi bagi kemudahan pemprosesan maklumat perlu disediakan dan dapat diakses dengan selamat.	
5.37.1 Pengendalian Prosedur Operasi	**Tanggungjawab**
Semua prosedur pengurusan operasi hendaklah dikenal pasti, didokumenkan, disimpan dan dihadkan capaian berdasarkan keperluan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur operasi hendaklah didokumenkan dengan jelas, teratur, dikemas kini dan sedia diguna pakai oleh pengguna; b) Setiap perubahan kepada prosedur operasi mestilah dikawal; c) Tugas dan tanggungjawab fungsi perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT; dan	i. ICTSO ii. Semua pentadbir sistem

d) Kemudahan ICT untuk kerja-kerja pembangunan, pengujian dan operasi perlu diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	

PERKARA 6.0 – KAWALAN SUMBER MANUSIA

KAWALAN 6.1 – SARINGAN	
Objektif: Memastikan semua sumber manusia termasuk pihak ketiga yang berkepentingan memahami tanggungjawab dan peranan, meningkatkan pengetahuan dalam aspek keselamatan ICT, mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
6.1.1 Sebelum Memulakan Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menjelaskan peranan dan tanggungjawab pihak yang terlibat dalam meningkatkan keselamatan penyampaian maklumat dan mengurangkan risiko penyalahgunaan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pihak yang terlibat selaras dengan keperluan perkhidmatan, mengikut peraturan sedia ada; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	i. ICTSO/ Pengurus ICT ii. Pengurus Sumber Manusia iii. Pengguna iv. Pihak Ketiga
KAWALAN 6.2 - TERMA DAN SYARAT PERJAWATAN	
Objektif: Memastikan semua sumber manusia termasuk pihak ketiga yang berkepentingan mempunyai kesedaran terhadap tanggungjawab dan ancaman keselamatan supaya segala dasar keselamatan dipatuhi dalam melaksanakan tugasan bagi menurunkan risiko akibat kesilapan manusia.	
6.2.1 Semasa Melaksanakan Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan pihak yang terlibat dengan Maklumat Rahsia Rasmi menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan;	i. ICTSO/ ii. Pengurus ICT/ iii. Pengurus Sumber Manusia/ iv. Pengguna/

b) Memastikan pihak yang terlibat mematuhi keselamatan siber berdasarkan kepada dasar dan peraturan yang ditetapkan oleh Kerajaan; c) Memastikan tindakan disiplin atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan; d) Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan siber dinyatakan dalam senarai tugas yang merangkumi: i. Tanggungjawab kakitangan; ii. Hubungan dengan pegawai atasan; dan iii. Tanggungjawab kakitangan dalam keselamatan siber.	v. Pihak Ketiga

KAWALAN 6.3 - KESEDARAN KESELAMATAN MAKLUMAT, PENDIDIKAN DAN LATIHAN

Objektif : Memastikan semua sumber manusia termasuk pihak ketiga yang berkepentingan diberikan kesedaran, pendidikan dan latihan berkaitan pengurusan keselamatan ICT dalam melaksanakan tugasan dan tanggungjawab mereka.

6.3.1 Kesedaran Keselamatan Maklumat	**Tanggungjawab**
a) Kakitangan haruslah diberi latihan yang bersesuaian dan berterusan dalam semua aspek keselamatan siber yang berkaitan dengan tugasan mereka; b) Kakitangan bertanggungjawab mengikuti latihan pengurusan keselamatan siber berdasarkan keperluan; c) Ketua Jabatan atau Ketua Bahagian bertanggungjawab mengkaji semula keperluan latihan untuk setiap kakitangan di bawahnya; d) Program kesedaran keselamatan siber juga perlu dilaksanakan secara berterusan sebagai langkah peringatan kepada kakitangan jabatan berkenaan kepentingan keselamatan ICT INSTUN; e) Mengikuti program kesedaran keselamatan siber secara berkala sekurang-kurangnya satu (1) kali setahun; dan	i. ICTSO/ Pengurus ICT ii. Pengurus Sumber Manusia iii. Pengguna iv. Pihak Ketiga

f) Memastikan kesedaran berkaitan Polisi Keselamatan Siber diberikan kepada kakitangan dan pihak ketiga.	
KAWALAN 6.4 – PROSES DISIPLIN	
Objektif: Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas pegawai yang terlibat sekiranya berlaku pelanggaran terhadap peraturan yang ditetapkan.	
6.4.1 Tindakan Disiplin	**Tindakan**
Memastikan adanya proses tindakan disiplin dan/ atau undang-undang ke atas kakitangan jabatan sekiranya berlaku pelanggaran terhadap peraturan yang ditetapkan.	i. Ketua Jabatan ii. Pengurus Sumber Manusia iii. Unit Integriti
KAWALAN 6.5 - TANGGUNGJAWAB SELEPAS PERTUKARAN ATAU TAMAT PERKHIDMATAN	
Objektif: Memastikan pertukaran atau tamat perkhidmatan semua pengguna dan pihak ketiga yang berkepentingan diuruskan dengan teratur.	
6.5.1 Pertukaran atau Tamat Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikembalikan kepada jabatan mengikut peraturan dan terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat mengikut peraturan yang ditetapkan.	i. ICTSO ii. Pengurus Sumber Manusia iii. Pentadbir Sistem iv. Pengguna v. Pihak Ketiga
KAWALAN 6.6 – PERJANJIAN KERAHSIAAN ATAU KETIADAAN PENDEDAHAN	
Objektif: Klausa kerahsiaan atau ketiadaan pendedahan maklumat sulit hendaklah dinyatakan dan diperakui oleh semua kakitangan jabatan dan pihak ketiga yang terikat dengan kontrak menjalankan tugasan di INSTUN. Syarat-syarat perjanjian kerahsiaan atau *Non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pihak ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	

6.6.1 Perjanjian Pemindahan dan Kerahsiaan Maklumat	Tanggungjawab
a) *Non-Disclosure Agreements* (NDA) perlu diwujudkan bagi memastikan kerahsiaan, integriti dan ketersediaan maklumat terpelihara semasa proses pemindahan maklumat dan perisian di antara INSTUN dengan agensi luar atau pihak ketiga yang berkaitan; dan b) Keperluan melindungi kerahsiaan meliputi integriti dan kerahsiaan maklumat hendaklah disemak dan didokumenkan.	i. Kakitangan Jabatan ii. Semua Pentadbir Sistem iii. Pihak Ketiga iv. Pengguna

KAWALAN 6.7 – KEMUDAHAN KERJA JARAK JAUH	
Objektif: Memastikan kawalan keselamatan maklumat terhadap individu yang bekerja jarak jauh untuk menghalang pendedahan maklumat dan capaian yang tidak sah serta salah guna kemudahan.	
6.7.1 Peralatan Mudah Alih dan Kerja Jarak Jauh	**Tanggungjawab**
Perkara yang perlu dipatuhi bagi memastikan keselamatan peralatan mudah alih dan kerja jarak jauh terjamin adalah seperti berikut: a) Kerja jarak jauh hanya boleh dilaksanakan setelah mendapat kelulusan pegawai yang diberi kuasa dan pemilik sistem yang berkaitan; b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; c) Memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; d) Menggalakkan penggunaan capaian Internet sendiri berbanding capaian Internet awam; e) Memastikan aset ICT dilengkapi dengan antivirus dan sentiasa dikemas kini; dan f) Tindakan perlindungan aset ICT mudah alih hendaklah diambil seperti menyimpan dan kunci di tempat yang selamat apabila tidak digunakan.	i. Ketua Jabatan ii. Pentadbir Aset ICT/ Pemilik Aset/ iii. Pengguna Aset

KAWALAN 6.8 - LAPORAN KES KESELAMATAN MAKLUMAT	
Objektif : Memastikan insiden dikendalikan dengan konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat bagi meminimumkan impak supaya tidak menjejaskan sistem penyampaian perkhidmatan.	
6.8.1 Pelaporan Insiden Keselamatan Maklumat	**Tanggungjawab**
a) Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada CSIRT. Semua maklumat adalah SULIT dan tidak boleh didedahkan tanpa kebenaran daripada ICTSO; ii. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; iii. Menyimpan jejak audit dan me-melihara bahan bukti; dan iv. Menyediakan dan melaksanakan pelan tindakan pemulihan. b) Prosedur pelaporan insiden keselamatan siber hendaklah berdasarkan Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam. c) Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT dengan kadar segera (rujuk Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Siber Sektor Awam): i. Maklumat didapati hilang, disyaki hilang, didedahkan oleh pihak-pihak yang diberi kuasa, atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;	i. ICTSO ii. CSIRT

ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; iii. Kata laluan atau mekanisme kawalan akses dicuri, didedahkan atau disyaki hilang; iv. Berlaku kejadian gangguan sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan v. Berlaku percubaan pencerobohan, penyelewengan dan insiden yang tidak dijangka yang boleh menjejaskan keselamatan siber.	
6.8.2 Pelaporan Kelemahan Keselamatan	**Tanggungjawab**
Kakitangan jabatan dan pihak ketiga yang menggunakan sistem dan perkhidmatan jabatan dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan ICT. Insiden keselamatan perlu dilaporkan apabila berlaku perkara seperti berikut: a) Kawalan keselamatan maklumat yang tidak berkesan; b) Pelanggaran sebarang kerahsiaan, integriti atau ketersediaan maklumat; c) Kesilapan manusia; d) Ketidakpatuhan terhadap polisi keselamatan maklumat; e) Pelanggaran keselamatan fizikal; f) Perubahan sistem yang tidak melalui proses pengurusan perubahan; g) Perisian atau perkakasan yang rosak atau tidak berfungsi; h) Penyalahgunaan hak akses; i) Kerentanan; dan j) Percubaan serangan perisian hasad.	i. ICTSO ii. CSIRT iii. Pengguna iv. Pihak Ketiga

PERKARA 7.0 – KAWALAN FIZIKAL

KAWALAN 7.1 - PERIMETER KESELAMATAN FIZIKAL

Objektif: Memastikan maklumat, premis dan kemudahan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

7.1.1 Keselamatan Fizikal	Tanggungjawab
Keselamatan fizikal adalah bertujuan untuk mengesan, menghalang, dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab; c) Memperkukuhkan dinding dan siling; d) Memasang alat penggera dan sistem CCTV; e) Mengehadkan laluan keluar masuk; f) Menyediakan kaunter kawalan; g) Menyediakan tempat atau bilik khas untuk pelawat; h) Mewujudkan perkhidmatan kawalan keselamatan; i) Mereka bentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau rusuhan; j) Merujuk garis panduan keselamatan untuk kakitangan jabatan yang bekerja di dalam kawasan terhad;	i. CGSO/ Pegawai Keselamatan ii. CDO/ ICTSO

k) Sistem kawalan kunci dengan menetapkan pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan l) Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan Kawasan terhad.	
7.1.2 Kawasan Terhad	**Tanggungjawab**
Kawasan terhad ditakrifkan sebagai kawasan di mana terdapat peralatan ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tiada kawalan. Kawalan dilaksanakan untuk melindungi peralatan ICT yang terdapat di dalam kawasan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut. a) Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja; b) Pihak ketiga tidak dibenarkan untuk memasuki kawasan terhad kecuali bagi yang telah mendapat kebenaran dan hendaklah diiringi sehingga tugas selesai; c) Peralatan media perakaman/ storan/ komunikasi adalah tidak dibenarkan dibawa masuk ke dalam pusat data, kecuali dengan kebenaran pegawai yang diberi kuasa; dan d) Aktiviti mengambil gambar, merakam video, Merekodkan kan suara atau penggunaan peralatan yang tidak berkenaan adalah dilarang.	i. CGSO ii. ICTSO iii. Pengguna iv. Pihak Ketiga v. Pelawat
KAWALAN 7.2 – KEMASUKAN FIZIKAL	
Objektif: Melaksanakan kawalan akses masuk kepada maklumat, premis dan kemudahan ICT.	
7.2.1 Kawalan Masuk Fizikal	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: **<u>Pengguna dan pelawat</u>**	i. Pengguna ii. Pelawat iii. CGSO

Setiap pengguna hendaklah memakai pas keselamatan sepanjang waktu bertugas; a) Setiap pelawat mestilah mendaftar dan mendapatkan pas pelawat di pintu masuk utama jabatan untuk ke kawasan/ tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; b) Semua pas keselamatan hendaklah diserahkan semula kepada jabatan apabila pengguna bertukar, berhenti atau bersara; c) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pegawai keselamatan jabatan.	

KAWALAN 7.3 – KESELAMATAN PEJABAT, BILIK DAN FASILITI

Objektif : Memastikan keselamatan dan perlindungan terhadap maklumat, premis dan peralatan ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan, kecuaian serta akses yang tidak dibenarkan.

7.3.1 Kawalan Persekitaran	**Tanggungjawab**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan semasa.	i. CGSO ii. ICTSO iii. Bahagian Pentadbiran

KAWALAN 7.4 – PEMANTAUAN KESELAMATAN FIZIKAL

Objektif : Memantau dan memastikan keselamatan fizikal dikawal untuk mengelakkan maklumat pengawasan seperti suapan video daripada diakses oleh individu yang tidak dibenarkan.

7.4.1 Pemantauan Kawasan Fizikal Premis	Tanggungjawab
Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti kamera litar tertutup (CCTV) dan perisian pengurusan maklumat keselamatan fizikal.	Bahagian Pentadbiran
KAWALAN 7.5 – PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN	
Objektif : Memastikan infrastruktur yang direka bentuk dilindungi daripada ancaman fizikal dan persekitaran.	
7.5.1 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran	**Tanggungjawab**
a) Kawalan dan perlindungan keselamatan ke atas kawasan ICT perlu mengambil kira ancaman fizikal, perbuatan manusia seperti serangan berniat jahat, kemalangan, rusuhan ataupun bencana alam dan kesan perubahan iklim seperti kebakaran, banjir, gempa bumi dan lain-lain. b) Agensi yang berkaitan perlu dirujuk bagi semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa dan mengubahsuai bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT. c) Bagi menjamin keselamatan persekitaran, Langkah-langkah berikut hendaklah dipatuhi: i. Merancang dan menyediakan pelan keseluruhan susun atur peralatan komputer, ruang atur pejabat dan sebagainya dengan teliti; ii. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	ICTSO/ Pengurus Khidmat Pengurusan / Pengurus Fasiliti

iii. Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dicapai dan dikendalikan; iv. Bahan mudah terbakar **DILARANG** disimpan di dalam kawasan penyimpanan aset ICT; v. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; vi. Pengguna adalah **DILARANG** merokok atau menggunakan peralatan yang boleh menyebabkan risiko kebakaran dan kerosakan kepada aset ICT; dan vii. Semua peralatan perlindungan keselamatan hendaklah diperiksa supaya sentiasa berada dalam keadaan tersedia.	

KAWALAN 7.6 – BEKERJA DI KAWASAN SELAMAT

Objektif: Memastikan maklumat dan peralatan ICT berada di dalam kawasan yang selamat daripada gangguan, ancaman atau kerosakan.

7.6.1 Keselamatan di Kawasan Bekerja	**Tanggungjawab**
Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: a) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di lokasi yang mempunyai ciriciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b) Akses adalah terhad kepada kakitangan jabatan yang telah diberi kuasa sahaja dan dipantau pada setiap masa; c) Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual;	i. Pengurus Khidmat Pengurusan ii. CGSO iii. Pentadbir Pusat Data

d) Butiran pelawat yang keluar masuk ke kawasan terhad perlu direkodkan; e) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan; f) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; dan g) Memperkukuh dinding, siling, tingkap dan pintu serta dikunci untuk mengawal kemasukan.	

KAWALAN 7.7 - DASAR MEJA KOSONG DAN SKRIN KOSONG (*CLEAR DESK AND CLEAR SCREEN POLICY*)

Objektif: Memastikan semua maklumat sensitif dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

7.7.1 Dasar Meja Kosong dan Skrin Kosong	**Tanggungjawab**
Dasar Meja Kosong dan Skrin Kosong bermaksud tidak meninggalkan maklumat sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b) Menetapkan paparan skrin akan tertutup selepas 10 minit jika tidak digunakan; c) Dokumen terperingkat hendaklah disimpan dalam laci atau kabinet fail yang berkunci; d) Memastikan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain di padam apabila tidak diperlukan lagi; dan e) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	i. Pengguna ii. Pentadbir Sistem (*Active Directory*)

KAWALAN 7.8 – PERLINDUNGAN DAN KEDUDUKAN PERALATAN	
Objektif: Melindungi peralatan ICT dari kehilangan, kerosakan, kecurian serta gangguan pada peralatan tersebut.	
7.8.1 Keselamatan Peralatan ICT	**Tanggungjawab**
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut: a) Pengguna mesti mendapat kebenaran daripada ICTSO atau pegawai yang dilantik untuk membuat instalasi perisian tambahan; b) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; c) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; d) Peralatan-peralatan kritikal seperti pelayan, peranti rangkaian, peranti keselamatan dan sistem pendingin hawa/ bekalan elektik perlu disokong oleh *Uninterruptible Power Supply* (UPS); e) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; f) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlu mendapat kelulusan pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan; g) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; h) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	i. ICTSO ii. Pegawai Aset iii. Pentadbir Sistem iv. Pengguna v. Pihak Ketiga

i) Pengguna mesti mendapat kebenaran daripada ICTSO atau pegawai yang diberikan kuasa untuk mengubah kedudukan peralatan ICT; j) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab; k) Sebarang Pelekat selain bagi tujuan rasmi tidak dibenarkan bagi menjamin peralatan tersebut sentiasa berkeadaan baik; l) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; m) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; n) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; o) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; p) Memastikan suis elektrik ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat; q) Memastikan pemulangan aset ICT mengikut peraturan dan terma yang ditetapkan; dan r) Membatalkan atau nyahaktif kebenaran dan capaian ke atas aset ICT mengikut peraturan dan terma yang ditetapkan.	

KAWALAN 7.9 – KESELAMATAN ASET DI LUAR PREMIS	
Objektif: Memastikan Aset ICT yang dibawa keluar dari premis dilindungi dan selamat dari risiko seperti kecurian, kerosakan dan lain-lain.	
7.9.1 Peralatan ICT di Luar Premis Jabatan	**Tanggungjawab**
Bagi peralatan ICT yang dibawa keluar dari premis, Langkah-langkah keselamatan berikut hendaklah diambil: a) Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran; b) Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar; c) Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; d) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian;	i. Pengguna ii. Pegawai Aset iii. Pihak Ketiga

KAWALAN 7.10 – MEDIA STORAN	
Objektif : Memastikan media storan berada dalam keadaan yang baik dan selamat supaya terjamin kerahsiaan, integriti dan ketersediaan untuk digunakan.	
7.10.1 Media Storan	**Tanggungjawab**
a) Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, *thumb drive, external drive* dan media storan lain. b) Tindakan berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan ketersediaan maklumat yang disimpan adalah terjamin dan selamat: i. Mewujudkan prosedur untuk mengendali dan menyimpan maklumat daripada didedah tanpa kebenaran atau disalah guna; ii. Media storan mudah alih yang di bawa keluar perlu mendapat kelulusan dan direkodkan; iii. Media storan mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-	i. Pengguna ii. Pentadbir Sistem

ciri keselamatan bersesuaian dengan kandungan maklumat; iv. Menggunakan teknik kriptografi sekiranya media storan mudah alih menyimpan maklumat rahsia rasmi; v. Memastikan media storan mudah alih boleh berfungsi sekiranya diperlukan; vi. Memastikan maklumat rahsia rasmi yang disimpan melebihi satu media storan mudah alih mengambil kira risiko kerosakan atau kehilangan maklumat; vii. Mendaftar media storan mudah alih untuk mengelakkan kehilangan maklumat; viii. Mengawal dan memantau penggunaan USB port untuk mengelakkan kebocoran atau pemindahan maklumat; ix. Memantau pemindahan maklumat ke media storan mudah alih; x. Memastikan keselamatan maklumat semasa penghantaran media storan mudah alih menggunakan pos; xi. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada Pengurus ICT dan pegawai yang dibenarkan sahaja; dan xii. Hanya maklumat rasmi dibenarkan untuk disimpan dalam media storan yang dibekalkan oleh jabatan c) Prosedur pelupusan dan penggunaan semula media storan hendaklah diwujudkan bagi mengurangkan risiko kebocoran maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: i. Media storan yang akan digunakan semula perlu di sanitasi atau di format terlebih dahulu;	

ii. Melupuskan media storan yang mengandungi maklumat rahsia rasmi menggunakan kaedah yang dibenarkan sekiranya tidak diperlukan lagi iii. Pelupusan media storan oleh pihak ketiga hendaklah mematuhi kawalan keselamatan dan dilaksanakan oleh pihak yang berpengalaman; iv. Pelupusan maklumat mengikut garis panduan yang dikeluarkan oleh Arkib Negara Malaysia; v. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan; vi. Pelupusan media storan hendaklah direkodkan; vii. Semua media storan yang hendak dilupuskan mestilah dirujuk kepada Bahagian yang bertanggungjawab berkaitan ICT; dan viii. Pengguna hendaklah menghapuskan atau memindahkan semua Maklumat rasmi/ terperingkat dari media storan sendiri apabila bersara/ bertukar jabatan/ ditamatkan perkhidmatan dan tamat/ ditamatkan kontrak.	

KAWALAN 7.11 – UTILITI SOKONGAN

Objektif: Memastikan bekalan kuasa dan semua utiliti sokongan berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk air, pendingin hawa, generator, alat komunikasi dan lain-lain.

7.11.1 Bekalan Kuasa	**Tanggungjawab**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut *voltage* yang bersesuaian; b) Peralatan sokongan seperti *Uninterruptible* Power *Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi	i. ICTSO ii. Penyelenggara Bangunan iii. Pengurus Fasiliti

perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	

KAWALAN 7.12 – KESELAMATAN PENGKABELAN

Objektif: Memastikan kabel rangkaian dan Peralatan ICT dilindungi daripada gangguan dan pencerobohan untuk mengelakkan maklumat terdedah. (kabel rangkaian & kabel peralatan ICT).

7.12.1 Kabel Rangkaian	**Tanggungjawab**
Kabel Peralatan ICT hendaklah dilindungi dengan langkahlangkah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel dengan menggunakan konduit untuk mengelakkan kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wiretapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	i. ICTSO ii. Pentadbir Rangkaian iii. Bahagian Pentadbiran iv. Pihak Ketiga

KAWALAN 7.13 – PENYELENGGARAAN PERALATAN

Objektif: Peralatan ICT hendaklah di selenggara dengan baik dan terkawal bagi memastikan ketersediaan, kerahsiaan dan integriti.

7.13.1 Penyelenggaraan Peralatan ICT	**Tanggungjawab**
Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan ketersediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi dan konfigurasi asal serta manual yang ditetapkan;	i. ICTSO ii. Pengguna iii. Pentadbir Sistem iv. Pihak Ketiga

b) Memastikan perkakasan hanya boleh di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada pengguna yang diberikan tanggungjawab menjaganya.	

KAWALAN 7.14 – PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

Objektif: Memastikan kaedah pelupusan atau penggunaan semula peralatan dilaksanakan secara teratur dan selamat mengikut peraturan yang berkuat kuasa supaya tidak berlaku kebocoran maklumat.

7.14.1 Pelupusan Peralatan Aset ICT	**Tanggungjawab**
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; b) Semua kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula;	i. Pegawai Aset ii. Pengguna

c) Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; d) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat salinan pendua; e) Peralatan ICT yang akan dilupuskan secara pindah-milik hendaklah dipastikan data-data dalam storan telah dihapus secara kekal dan selamat; f) Peralatan yang hendak dilupuskan mestilah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; g) Pegawai aset bertanggungjawab merekodkan kan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Inventori; h) Pegawai aset bertanggungjawab Merekodkan kan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori; dan i) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk drives*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian di jabatan; iii. Memindah keluar dari jabatan mana-mana peralatan ICT yang hendak dilupuskan; dan	

iv.	Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Bahagian Pentadbiran Jabatan.	

PERKARA 8.0 – KAWALAN TEKNOLOGI

KAWALAN 8.1 – PERANTI AKHIR PENGGUNA (*USER ENDPOINT DEVICES*)	
Objektif: Melindungi maklumat yang terdapat dalam peranti akhir pengguna	
8.1.1 Peranti Akhir Pengguna	**Tanggungjawab**
Perkara yang perlu dipatuhi bagi memastikan keselamatan peranti akhir pengguna adalah seperti berikut: a) Memastikan jenis dan klasifikasi maklumat yang boleh diakses, diproses atau disimpan dalam Aset ICT pengguna; b) Memastikan semua Aset ICT pengguna didaftarkan; c) Memastikan pengguna bertanggungjawab ke atas Aset ICT; d) Memastikan perisian yang boleh dipasang pada Aset ICT pengguna telah mendapat kelulusan; e) Memastikan Aset ICT pengguna dikonfigurasikan dengan versi perisian atau *patches* terkini; f) Menetapkan peraturan bagi sambungan ke rangkaian awam, atau rangkaian lain di luar premis menggunakan Aset ICT pengguna; g) Mematuhi kawalan capaian menggunakan Aset ICT pengguna; h) Melaksanakan enkripsi bagi penyimpanan maklumat jabatan sekiranya perlu; i) Memastikan Aset ICT pengguna mempunyai perisian *endpoint security*; j) Memastikan peraturan berkaitan *remote disabling, deletion or lockout* di patuhi; k) Memastikan pelaksanaan sandaran bagi maklumat jabatan yang disimpan di dalam Aset ICT pengguna; l) Menggunakan perkhidmatan web dan aplikasi yang dibenarkan sahaja;	i. ICTSO ii. Pentadbir Rangkaian ICT iii. Pentadbir Pusat Data iv. Pentadbir Aset ICT v. Pemilik Aset vi. Pengguna Aset

m) Melaksanakan analisa penggunaan Aset ICT pengguna; n) Menyahaktifkan *USB port* sekiranya perlu; o) Memastikan pengasingan (*hard disk partition*) data dan perisian pada Aset ICT pengguna; dan p) Jabatan berhak untuk mengambil tindakan tatatertib yang sesuai seperti penamatan akses sekiranya didapati tidak mematuhi peraturan dalam polisi ini.	
8.1.2 *Bring Your Own Device (BYOD)*	**Tanggungjawab**
BYOD merupakan Aset ICT/ peralatan mudah alih persendirian seperti telefon pintar, *tablet* dan *laptop* yang digunakan oleh pengguna yang melaksanakan tugas rasmi melalui sambungan rangkaian jabatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengasingkan penggunaan bagi tujuan peribadi dan tugasan rasmi. Instalasi perisian yang dibekalkan oleh jabatan pada Aset ICT/ peralatan mudah alih persendirian hendaklah mendapatkan kelulusan; b) Membenarkan akses kepada maklumat yang berkaitan dengan tugasan rasmi dan menghapuskan data rahsia rasmi pada Aset ICT/ peralatan mudah alih persendirian apabila tidak digunakan lagi; c) Memastikan hak harta intelek adalah di bawah tanggungjawab pengguna Aset ICT/ peralatan mudah alih persendirian; d) Penyalahgunaan Aset ICT/ peralatan mudah alih persendirian adalah di bawah tanggungjawab pengguna sendiri; e) Jabatan tidak bertanggungjawab ke atas sebarang kerosakan sistem operasi atau perkakasan Aset ICT/ peralatan mudah alih persendirian; dan	Semua

f) Jabatan menghormati privasi Aset ICT/ peralatan mudah alih persendirian dengan mengambil langkah pencegahan yang terbaik untuk memastikan keselamatan maklumat. Jabatan mempunyai hak untuk menjejaki dan meminta akses kepada Aset ICT/ peralatan mudah alih persendirian sekiranya terdapat pelanggaran keselamatan maklumat yang dikenal pasti.	
8.1.3 Tanggungjawab Pengguna	**Tanggungjawab**
Pengguna perlu memastikan mana-mana peranti akhir pengguna mematuhi ciri-ciri keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menamatkan sesi aktif apabila selesai tugas; b) Mengaktifkan kawalan yang bersesuaian seperti *password protected screen saver*; c) *Log-off* pelayan dan komputer pejabat apabila sesi bertugas selesai; dan d) Melindungi Aset ICT daripada kecurian atau kecuaian.	Semua
8.1.4 Sambungan Rangkaian Tanpa Wayar Untuk Peranti Akhir Pengguna	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Konfigurasi rangkaian tanpa wayar untuk melindungi daripada protokol yang mempunyai kelemahan; b) Menetapkan *bandwidth* rangkaian yang bersesuaian bergantung kepada jenis akses; c) Tidak mendedahkan identiti dan kata laluan sambungan rangkaian tanpa wayar; dan d) Jabatan digalakkan menggunakan *Network Access Control* (NAC).	Pentadbir Rangkaian ICT

KAWALAN 8.2 – HAK AKSES ISTIMEWA	
Objektif: Memastikan akses pengguna, komponen servis dan perisian diberikan kepada pengguna yang dibenarkan sahaja.	
8.2.1 Maklumat Hak Akses	**Tanggungjawab**
Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang berikut: a) Mengenal pasti pengguna yang memerlukan hak akses untuk sistem aplikasi, sistem pengoperasian dan pengurusan pangkalan data; b) Menetapkan hak akses kepada pengguna yang memerlukan atau berdasarkan permohonan mengikut keperluan; c) Memantau secara berkala kepada hak akses dan rekod hak akses yang diberikan; d) Menetapkan pelaksanaan tempoh tamat hak akses yang diberikan; e) Memastikan pengguna mengetahui tanggungjawab hak akses yang diterima; f) Memastikan perbezaan peranan akses untuk pentadbir dan pengguna; g) Sekiranya berlaku perubahan struktur organisasi, penetapan dan penggunaan ke atas hak akses perlu disemak semula berdasarkan keperluan skop tugas; h) Memastikan penggunaan ID pentadbir tidak generik atau melambangkan peranan *super user* seperti *root* dan *administrator*; i) Memberikan hak akses sementara untuk perubahan atau penyelenggaraan yang dilaksanakan oleh pihak ketiga; j) Merekodkan semua log masuk untuk kegunaan jejak	i. ICTSO ii. Pentadbir Sistem Aplikasi iii. Pentadbir Rangkaian ICT iv. Pentadbir Pusat Data

audit; k) Tidak berkongsi ID pengguna dengan orang lain; l) Menggunakan ID pengguna berdasarkan skop tugas (melaksanakan tugasan harian) dan tidak menggunakan ID pentadbir; dan m) Sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan.	
KAWALAN 8.3 – SEKATAN AKSES MAKLUMAT *(INFORMATION ACCESS RESTRICTION)*	
Objektif: Memastikan hanya akses yang dibenarkan ke atas maklumat dan aset yang berkaitan.	
8.3.1 Akses Maklumat dan Aset Yang Berkaitan	**Tanggungjawab**
Bagi memastikan kawalan had akses ke atas maklumat dan aset yang berkaitan, perkara berikut hendaklah dipatuhi: a) Tidak membenarkan akses ke maklumat rahsia rasmi bagi pengguna yang tidak dibenarkan; b) Menyediakan konfigurasi untuk mengawal akses maklumat di dalam sistem, aplikasi dan perkhidmatan; c) Mengawal data yang boleh diakses mengikut kategori pengguna; d) Mengawal individu dan kumpulan yang telah dikenal pasti yang mempunyai akses seperti *read, write, delete* dan *execute*; e) Menyediakan kawalan fizikal atau kawalan hak akses untuk aplikasi kritikal, aplikasi data atau sistem; f) Setiap aktiviti akses ke atas maklumat hendaklah direkodkan (log); g) Mengehadkan hak akses sistem aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun pengguna akan disekat; dan h) Akses maklumat di luar premis pejabat adalah tidak digalakkan. Walau bagaimanapun, penggunaannya	i. ICTSO ii. Pentadbir Sistem

terhad kepada perkhidmatan yang diberi kebenaran sahaja.	
8.3.2 Akses Maklumat Rahsia Rasmi	**Tanggungjawab**
Untuk melindungi maklumat rahsia rasmi yang kritikal, pengurusan akses perlu mematuhi perkara berikut: a) Melaksanakan kawalan untuk akses maklumat mengikut tempoh masa yang dibenarkan; b) Melaksanakan kawalan untuk akses maklumat yang diberikan kepada pihak ketiga; c) Memantau dan menguruskan semua penggunaan atau penyebaran maklumat secara *real-time*; d) Maklumat hendaklah dilindungi daripada perubahan, penyalinan dan pengedaran yang tidak dibenarkan (termasuk percetakan); dan e) Merekodkan kan sebarang perubahan ke atas maklumat tersebut.	i. ICTSO ii. Pentadbir Sistem
8.3.3 Kawalan Pengurusan Akses Maklumat dan Aset Yang Berkaitan	**Tanggungjawab**
Untuk melindungi maklumat semasa proses pewujudan, pemprosesan, penyimpanan, penghantaran dan pelupusan adalah seperti berikut: a) Menetapkan kawalan mengenai pengurusan akses seperti berikut: i. Memberikan kebenaran akses berdasarkan identiti, peranti, lokasi atau aplikasi; ii. Menetapkan klasifikasi maklumat yang perlu dilindungi. b) Mewujudkan proses operasi, pemantauan dan pelaporan serta menyokong infrastruktur teknikal; c) Mendapatkan pengesahan dan kebenaran untuk mengakses maklumat; d) Mengehadkan akses seperti mempunyai had masa yang dibenarkan;	i. ICTSO ii. Pentadbir Sistem iii. Pegawai Aset

e) Menggunakan enkripsi untuk melindungi maklumat jika berkaitan; f) Menetapkan kebenaran untuk mencetak maklumat; g) Merekodkan kan log akses kepada maklumat dan tujuan maklumat digunakan; dan h) Menghantar pemakluman jika terdapat insiden penyalahgunaan maklumat.	
KAWALAN 8.4 – AKSES KEPADA KOD SUMBER	
Objektif: Akses kepada kod sumber dan mod pembangunan hendaklah dikawal. Ini adalah untuk mengelakkan perubahan yang tidak dibenarkan bagi mengekalkan kerahsiaan harta intelek ICT.	
8.4.1 Kawalan Capaian kepada Kod Sumber (*Source Code*)	**Tanggungjawab**
Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan. Perkara berikut perlu dipatuhi untuk mengawal akses kepada kod sumber bagi meminimumkan potensi kegagalan sistem aplikasi: a) Menguruskan akses kepada kod sumber dan program *source libraries* berdasarkan prosedur yang ditetapkan; b) Membenarkan akses *read* dan *write* mengikut kebenaran dan menguruskan risiko penyalahgunaan kod sumber; c) Pengemaskinian kod sumber serta pemberian akses kepada kod sumber perlu mematuhi prosedur kawalan perubahan yang diluluskan; d) Tidak membenarkan Pihak Ketiga akses secara terus kepada repositori kod sumber tetapi melalui perisian pembangunan yang mengawal aktiviti dan kebenaran kepada kod sumber; e) Menyimpan senarai kod sumber di tempat selamat dan memberikan kawalan akses kepada individu yang dibenarkan; dan	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem Aplikasi iv. Pihak Ketiga

f) Menyimpan log audit akses dan perubahan kepada kod sumber.	
KAWALAN 8.5 – PENGESAHAN YANG SELAMAT (*SECURE AUTHENTICATION*)	
Objektif: Memastikan pengguna atau individu menggunakan akses yang sah dan selamat ke atas sistem aplikasi dan perkhidmatan yang disediakan.	
8.5.1 Pengesahan Prosedur Log Masuk Yang Selamat	**Tanggungjawab**
Menyediakan kaedah yang sesuai atau terkini untuk pengesahan capaian (*authentication*). Prosedur log masuk perlu mematuhi perkara seperti berikut: a) Memaparkan maklumat hanya selepas log masuk berjaya; b) Memaparkan notis amaran sistem hanya boleh diakses oleh pengguna yang sah; c) Memaparkan *error handling* yang standard bagi semua ralat; d) Mengesahkan maklumat identiti yang dikunci masuk (*key- in*) untuk log masuk mencukupi dan betul; e) Melindungi ID pengguna dan kata laluan daripada cubaan log masuk *brute force*; f) Merekodkan kan jejak audit log masuk yang berjaya dan gagal; g) Menghantar notis keselamatan jika ada potensi percubaan atau pencerobohan ke atas log masuk yang dikesan; h) Memaparkan atau menghantar maklumat selepas akses masuk berjaya seperti di bawah: i. Tarikh dan masa berjaya akses; ii. Maklumat rekod bagi akses yang berjaya dan gagal ke sistem. i) Tidak memaparkan kata laluan semasa log masuk; j) Tidak menghantar kata laluan dalam *clear text* melalui rangkaian;	i. ICTSO ii. Pentadbir Sistem Aplikasi

k) Menamatkan sesi yang tidak aktif dalam tempoh masa yang ditetapkan; dan l) Mengehadkan tempoh masa sambungan bagi sistem yang kritikal. m) *Log-on* ke atas sistem pengoperasian perlu melalui satu kaedah yang selamat seperti *AD Authentication* bagi mengurangkan akses yang tidak dibenarkan.	

KAWALAN 8.6 – PENGURUSAN KAPASITI (*CAPACITY MANAGEMENT*)

Objektif : Memastikan pengurusan kapasiti ke atas kemudahan pemprosesan maklumat (sumber ICT), sumber manusia, keperluan pejabat dan lain-lain dikenal pasti.

8.6.1 Pengurusan Kapasiti	**Tanggungjawab**
Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. Perkara seperti berikut perlu diambil kira: a) Keperluan kapasiti hendaklah dirancang, diurus dan dikawal dengan terperinci bagi memastikan keperluannya adalah mencukupi serta bersesuaian untuk pembangunan dan operasi semasa atau pada masa akan datang. b) Keperluan kapasiti perlu mengambil kira ciri-ciri keselamatan bagi meminimumkan risiko gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. c) Pemantauan kapasiti sistem ICT perlu dilaksanakan untuk memastikan ketersediaan dan kecekapan sistem. d) Pengujian tekanan (*stress test*) ke atas sistem dan perkhidmatan hendaklah dilaksanakan untuk	i. Ketua Jabatan ii. Pentadbir Sistem

memastikan kapasiti mencukupi terutamanya semasa waktu puncak; dan e) Dokumen pengurusan kapasiti sumber perlu disediakan terutamanya untuk sistem kritikal.	
8.6.2 Peningkatan Kapasiti	**Tanggungjawab**
Keperluan peningkatan kapasiti perlu mengambil kira perkara berikut: a) Mewujudkan lantikan baharu; b) Mendapatkan kemudahan dan ruang kerja baharu; c) Melaksanakan perolehan yang berkaitan sistem pemprosesan, memori dan storan; dan d) Menggunakan pengkomputeran awan (*cloud computing*) sekiranya memenuhi keperluan semasa.	i. Ketua Jabatan ii. Pengurus ICT iii. ICTSO iv. Pentadbir Pusat Data
8.6.3 Pengurangan Kapasiti	**Tanggungjawab**
Perkara berikut perlu dipatuhi untuk mengurangkan kapasiti sumber: a) Menghapuskan data yang tidak digunakan lagi tertakluk kepada peraturan / pekeliling semasa yang berkuat kuasa; b) Melupuskan rekod fizikal tertakluk kepada peraturan / pekeliling semasa yang berkuat kuasa; c) Melupuskan sistem aplikasi, pangkalan data atau perkhidmatan ICT yang tidak digunakan lagi; d) Mengoptimumkan proses *batch* dan *scheduler*; e) Mengoptimumkan kod aplikasi dan kuiri pangkalan data; dan f) Mengehadkan *bandwidth* bagi perkhidmatan ICT yang menggunakan kapasiti tinggi.	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem
KAWALAN 8.7 – PERLINDUNGAN DARIPADA PERISIAN HASAD (*MALWARE*)	
Objektif: Memastikan perisian dan aset berkaitan ICT dilindungi daripada perisian hasad (*malware*). Perlindungan terhadap perisian hasad hendaklah berdasarkan	

maklumat pengesanan dan pembaikan perisian hasad tersebut, kesedaran keselamatan, akses sistem yang sesuai serta kawalan pengurusan perubahan.	
8.7.1 Perlindungan dari Perisian Hasad	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Melaksanakan kawalan untuk mencegah dan mengesan perisian yang tidak sah. b) Melaksanakan kawalan untuk mencegah dan mengesan laman web yang tidak diketahui dan disyaki tidak selamat; c) Mengurangkan kelemahan yang boleh dieksploitasi oleh perisian hasad; d) Melaksanakan pengesahan ke atas perisian dan maklumat sistem secara berkala terutamanya yang melibatkan sistem kritikal; e) Mewujudkan langkah-langkah perlindungan terhadap risiko daripada fail dan perisian yang diperolehi sama ada melalui rangkaian luar atau pada mana-mana medium lain; f) Memastikan perisian keselamatan yang digunakan sentiasa dikemas kini untuk mengimbas komputer dan media storan elektronik. Pengimbasan yang dilaksanakan merangkumi: i. Mengimbas sebarang data yang diterima melalui rangkaian atau melalui sebarang bentuk media storan elektronik sebelum digunakan; ii. Mengimbas lampiran yang dimuat turun sebelum digunakan; iii. Mengimbas laman web yang diakses; g) Menetapkan konfigurasi perisian keselamatan untuk mengesan ancaman risiko seperti:	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem iv. Pengguna

i. Polisi berdasarkan amalan terbaik (*best practise*); ii. Teknik untuk menyekat serangan perisian hasad. h) Melindungi daripada serangan perisian hasad semasa proses penyelenggaraan;	
i) Memberi kebenaran secara sementara atau kekal untuk menutup perisian pengesanan serangan hasad sekiranya ianya mengganggu operasi harian dengan mendapatkan kelulusan dan direkodkan; j) Menyediakan pelan kesinambungan perkhidmatan untuk proses pemulihan dari serangan *malware*, termasuklah data dan perisian *backup*. k) Mengasingkan persekitaran yang berisiko akan menghadapi bencana; l) Menyediakan prosedur kawalan serangan perisian hasad termasuk latihan, proses pemulihan dan pelaporan; m) Menyediakan program kesedaran atau latihan mengenai ancaman perisian berbahaya dan cara mengendalikannya; n) Melaksanakan pengumpulan maklumat perisian hasad yang terkini untuk langkah-langkah pencegahan; o) Mengesahkan maklumat yang berkaitan dengan serangan hasad daripada sumber yang sahih; dan p) Memasukkan klausa tanggungan dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.	

KAWALAN 8.8 – PENGURUSAN KE ATAS KERENTANAN TEKNIKAL (*MANAGEMENT OF TECHNICAL VULNERABILITIES*)	
Objektif: Mencegah eksploitasi kerentanan teknikal dalam sistem maklumat. Maklumat mengenai kelemahan teknikal perlu dikenal pasti, kelemahan organisasi perlu dinilai dan langkah-langkah yang sesuai perlu diambil.	
8.8.1 Mengenal Pasti Kerentanan Teknikal	**Tanggungjawab**
Jabatan hendaklah mempunyai inventori aset yang lengkap untuk pengurusan kerentanan teknikal yang berkesan. Inventori aset hendaklah mengandungi maklumat sistem seperti nama sistem, perisian dan versi yang digunakan serta pemilik yang bertanggungjawab ke atas perisian tersebut. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menetapkan peranan dan tanggungjawab untuk mengurus kerentanan teknikal seperti penilaian risiko, pengemaskinian *patches* dan lain-lain; b) Mengenal pasti sumber maklumat yang akan digunakan untuk mengesan kerentanan teknikal yang berkaitan dan sentiasa mengemas kini senarai aset sekiranya ada perubahan teknologi atau perisian yang digunakan; c) Memastikan kandungan kontrak perjanjian dengan pihak ketiga merangkumi laporan, pengurusan dan pendedahan kerentanan teknikal yang berkaitan; d) Menjalankan pengujian keselamatan untuk mengenal pasti kerentanan yang ada dan memastikan baik pulih dilaksanakan; e) Merancang, merekodkan, dan menguji penilaian keselamatan secara berkala oleh kakitangan atau pihak ketiga yang berkelayakan; f) Memastikan keselamatan penggunaan *libraries* dan kod sumber luar; dan	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek

g) Menilai tahap pendedahan bagi mengenal pasti tahap risiko	
8.8.2 Penilaian Kerentanan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Menganalisis dan mengesahkan laporan pengujian penilaian keselamatan. b) Mengenal pasti risiko dan mengambil Tindakan pemulihan ke atas penemuan daripada pengujian keselamatan yang telah dilaksanakan.	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek
8.8.3 Panduan Menangani Kerentanan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengambil tindakan yang bersesuaian mengikut tempoh masa yang ditetapkan setelah kelemahan dikenal pasti. b) Tindakan mengatasi kelemahan teknikal berdasarkan kategori risiko merujuk kepada pengurusan perubahan atau prosedur pengurusan pengendalian insiden keselamatan yang berkuat kuasa; c) Menggunakan-perisian asli; d) Menguji dan menilai pengemaskinian *patches* yang telah dilaksanakan sebelum dipasang pada persekitaran sebenar; e) Memastikan *patches* sentiasa dikemas kini terutamanya kepada sistem kritikal di Jabatan; f) Menguji keberkesanan ke atas tindakan pemulihan yang telah dilaksanakan; g) Sekiranya pengemaskinian tidak berjaya dilaksanakan, kawalan berikut perlu dipatuhi: i. Menggunakan cadangan lain yang diberikan oleh sumber yang sahih; ii. Menutup perkhidmatan yang terdedah kepada kelemahan teknikal;	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek

iii. Menambah polisi kawalan akses di segmen rangkaian;	
KAWALAN 8.9 – PENGURUSAN KONFIGURASI	
Objektif : Memastikan konfigurasi perkakasan, perisian, perkhidmatan, dan rangkaian ICT berfungsi dengan baik dan mengambil kira aspek keselamatan.	
8.9.1 Pengurusan Konfigurasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan konfigurasi semua perkhidmatan dan perkakasan ditetapkan mengikut keperluan; dan b) Peranan, tanggungjawab dan prosedur perlu disediakan untuk memastikan kawalan ke atas perubahan konfigurasi.	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek
8.9.2 Amalan Baik (*Best Practise*)	**Tanggungjawab**
Templat standard untuk konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian perlu disediakan seperti berikut: a) Menggunakan panduan umum atau amalan terbaik yang tersedia; b) Mempertimbangkan tahap perlindungan yang diperlukan untuk menentukan tahap keselamatan yang mencukupi; c) Menyokong dasar keselamatan maklumat yang sedang berkuat kuasa; dan d) Mempertimbangkan keupayaan dan kebolehgunaan konfigurasi keselamatan mengikut keperluan. Templat ini perlu disemak mengikut keperluan dan dikemas kini apabila ancaman atau kelemahan baharu dikenal pasti atau sekiranya terdapat versi perisian dan perkakasan baharu. Perkara berikut perlu dipatuhi dalam membangunkan templat: a) Meminimumkan bilangan had akses pentadbir;	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek

b) Menutup akses pengguna yang tidak diperlukan, tidak digunakan dan tidak selamat; c) Menutup atau menyekat perkhidmatan yang tidak diperlukan; d) Menyekat capaian kepada program utiliti (contoh: *anydesk*, *ip scanner*, *putty* dan lain-lain) dan tetapan konfigurasi; e) Penyeragaman masa (*clock synchronization*); f) Menukar kata laluan asal selepas proses instalasi dan penyemakan parameter keselamatan; g) Menyediakan *log off* secara automatik mengikut tempoh yang ditetapkan; dan h) Mematuhi terma dan syarat penggunaan lesen.	
8.9.3 Perubahan Konfigurasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian yang ditetapkan perlu direkodkan dan log perubahan konfigurasi perlu direkodkan; b) Perubahan pada konfigurasi harus mengikuti proses pengurusan perubahan yang telah diluluskan; dan c) Rekod konfigurasi perlu mengandungi: i. maklumat terkini pemilik; ii. tarikh terkini perubahan konfigurasi; iii. versi templat konfigurasi; iv. tetapan integrasi dengan aset lain.	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek
8.9.4 Pemantauan Konfigurasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Konfigurasi perlu dipantau dan disemak secara berkala bagi pengesahan tetapan konfigurasi, menilai kata	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek

laluan yang digunakan dan menilai aktiviti yang dijalankan; b) Sebarang perbezaan tanpa kebenaran daripada konfigurasi asal hendaklah ditukar semula sama ada secara automatik atau manual sebagai tindakan pembetulan; dan c) Maklumat konfigurasi adalah terhad dan hanya boleh diakses oleh pengguna yang dibenarkan sahaja.	

KAWALAN 8.10 – PENGHAPUSAN MAKLUMAT (*INFORMATION DELETION*)

Objektif : Memastikan maklumat sensitif tidak terdedah kepada pihak yang tidak sepatutnya dan penghapusan maklumat perlu memenuhi keperluan pekeliling dan peraturan semasa yang berkuat kuasa.

8.10.1 Penghapusan Data dan Maklumat	**Tanggungjawab**
Data dan maklumat yang disimpan di dalam pelayan, cakera keras, rangkaian, USB atau media storan yang lain hendaklah dihapuskan setelah ia tidak diperlukan lagi. Ini termasuklah data yang disimpan oleh pengguna dan Pihak Ketiga. Perkara berikut hendaklah dipatuhi semasa menghapus maklumat pada sistem, aplikasi dan perkhidmatan: a) Memilih kaedah penghapusan yang sesuai; b) Merekodkan keputusan penghapusan sebagai bukti; c) Bukti penghapusan maklumat perlu disediakan oleh pembekal sekiranya menggunakan perkhidmatan pembekal untuk penghapusan maklumat; dan d) Memastikan klausa penghapusan maklumat dimasukkan dalam perjanjian bersama Pihak Ketiga bagi memastikan penguatkuasaan semasa dan selepas penamatan perkhidmatan.	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek iv. Pihak Ketiga

8.10.2 Kaedah Penghapusan Data dan Maklumat	Tanggungjawab
Kaedah penghapusan data dan maklumat perlu dipatuhi berdasarkan pekeliling dan peraturan semasa yang berkaitan. Maklumat sensitif perlu dihapuskan sekiranya tidak diperlukan lagi mengikut kaedah berikut: a) Pengemaskinian konfigurasi sistem perlu dilaksanakan untuk memastikan maklumat yang tidak diperlukan dihapuskan secara selamat; b) Menghapuskan versi, salinan dan fail sementara yang tidak boleh digunakan lagi; c) Menggunakan pembekal yang diluluskan dan diperakui untuk melaksanakan perkhidmatan pelupusan; d) Menggunakan perisian yang diiktiraf untuk pelupusan maklumat; e) Menggunakan kaedah yang bersesuaian untuk melupuskan media storan; f) Penyedia perkhidmatan pengkomputeran awan perlu menyediakan *features* bagi memastikan penghapusan maklumat dapat dilaksanakan; dan g) media storan perlu dikeluarkan atau di sanitasi atau data dihapuskan untuk mengelakkan maklumat sensitive terdedah semasa peralatan dipulangkan semula kepada pembekal.	i. ICTSO ii. Pentadbir Sistem Aplikasi iii. Pentadbir Pusat Data iv. Pembantu Pegawai Aset v. Pengurus Projek

KAWALAN 8.11 – PENYAMARAN DATA (*DATA* MASKING)	
Objektif: Memastikan paparan data sensitif dihadkan mengikut keperluan organisasi , peraturan dan undang-undang semasa.	
8.11.1 Penyamaran Data	**Tanggungjawab**
Teknik untuk penyamaran data dalam sistem aplikasi atau peralatan termasuk: a) Enkripsi (Pengguna yang mempunyai *decryption key* sahaja boleh melihat data tersebut); atau	i. Pentadbir Sistem Aplikasi ii. Pentadbir Pangkalan Data iii. Pengurus Projek

b) Menggantikan data dengan "*Null*" atau menghapuskan salah satu huruf/ nombor (menghalang pengguna yang tidak dibenarkan untuk melihat mesej penuh); atau c) Mengubah nombor atau tarikh dari nilai sebenarnya; atau d) Penggantian data (menukar satu nilai kepada yang lain untuk menyembunyikan data sensitif); atau e) Menukar nilai dengan nilai *hash* (*hash value*).	
8.11.2 Pelaksanaan Penyamaran Data	**Tanggungjawab**
Semasa melaksanakan penyamaran data, perkara berikut perlu dipatuhi: a) Tidak semua data diberikan akses kepada pengguna. Sistem aplikasi atau peralatan hanya memaparkan data minimum kepada pengguna; b) Keperluan perundangan atau peraturan semasa yang berkuat kuasa hendaklah dipatuhi seperti penyamaran maklumat kad pembayaran semasa pemprosesan atau penyimpanan; c) Menyediakan kawalan akses kepada data yang diproses; dan d) Menyediakan jejak audit untuk Merekodkan penyediaan dan penerimaan data yang diproses.	i. Pentadbir Sistem Aplikasi ii. Pentadbir Pangkalan Data iii. Pengurus Projek
KAWALAN 8.12 – PENCEGAHAN KEBOCORAN DATA (*DATA LEAKAGE PREVENTION*)	
Objektif: Memastikan kebocoran data dikenal pasti dan dihalang daripada berlaku. Langkah pencegahan kebocoran data hendaklah digunakan pada sistem, rangkaian dan perkakasan ICT lain yang memproses, menyimpan atau menghantar maklumat.	
8.12.1 Pencegahan dan Pengesanan Kebocoran Data	**Tanggungjawab**
Perkara yang perlu dilaksanakan adalah seperti berikut: a) Mengenal pasti dan mengklasifikasikan maklumat untuk melindungi kebocoran maklumat seperti data peribadi; b) Memantau punca atau saluran kebocoran data;	i. Pentadbir Sistem Aplikasi ii. Pentadbir Keselamatan

c) Langkah pencegahan untuk mengelakkan kebocoran data; d) Organisasi perlu mengehadkan capaian pengguna; dan e) Memastikan proses sandaran maklumat dilindungi seperti penyulitan *(encryption)* dan kawalan akses.	iii. Pengurus Projek
8.12.2 Penggunaan Perisian Pencegahan Kebocoran Data (DLP)	**Tanggungjawab**
Perisian pencegahan kebocoran data adalah digalakkan untuk tujuan mengelakkan kebocoran data berlaku. Keperluan penggunaan perisian ini adalah seperti berikut: a) Mengenal pasti dan memantau maklumat sensitif yang berisiko diakses; b) Mengesan maklumat sensitif yang terdedah; c) Menyekat pengguna daripada rangkaian yang boleh mengakses maklumat sensitif; dan d) Mampu untuk Mengenal pasti data, memantau penggunaan dan pergerakan data serta mengambil tindakan untuk mencegah kebocoran data seperti memberi peringatan kepada pengguna.	iii. ICTSO iv. Pentadbir Keselamatan v. Pentadbir Sistem Aplikasi vi. Pentadbir Pangkalan Data vii. Pengurus Projek
KAWALAN 8.13 – SANDARAN MAKLUMAT (*BACK-UP*)	
Objektif: Memastikan salinan sandaran maklumat, perisian, konfigurasi dan sistem diselenggara serta diuji secara berkala.	
8.13.1 Pengurusan Sandaran	**Tanggungjawab**
Melaksanakan proses sandaran dan pemulihan sama ada maklumat di persekitaran *development*, *staging*, *production*, persekitaran *disaster recovery centre* atau lokasi yang dibenarkan perlu memastikan perkara berikut dipatuhi: a) Memastikan prosedur sandaran dan pemulihan direkodkan dengan lengkap;	i. ICTSO ii. Pentadbir Pusat Data iii. Pentadbir Sistem Aplikasi

b) Memastikan keperluan keselamatan maklumat bagi proses sandaran dan pemulihan dipenuhi ke atas semua sistem jabatan yang telah dikenal pasti; c) Memastikan salinan sandaran disimpan di lokasi dan jarak yang selamat untuk mengelakkan sebarang kerosakan akibat bencana di persekitaran *production*; d) Memastikan perlindungan yang sesuai diberikan ke atas maklumat sandaran selari dengan persekitaran *production*; e) Menguji sistem sandaran dan pemulihan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila perlu digunakan; f) Memastikan maklumat lengkap dan mencukupi sebelum proses sandaran dijana; g) Menetapkan tempoh simpanan maklumat sandaran yang disimpan dan maklumat tersebut perlu dihapus setelah melepasi tempoh yang ditetapkan; h) Menyediakan prosedur pengurusan sandaran dan pemulihan; i) Membuat salinan pendua ke atas semua maklumat dan sistem perisian mengikut jadual yang ditetapkan atau apabila berlaku perubahan versi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; dan j) Menyimpan salinan pendua sekurang-kurangnya di dalam satu (1) media storan yang berasingan.	
KAWALAN 8.14 – KELEWAHAN KEMUDAHAN PEMPROSESAN MAKLUMAT (*REDUNDANCY OF INFORMATION PROCESSING FACILITIES*)	
Objektif: Memastikan ketersediaan kemudahan operasi ICT.	
8.14.1 Kelewahan (*Redundancy*) Kemudahan Pemprosesan Maklumat	**Tanggungjawab**

Jabatan perlu Mengenal pasti dan Mereka bentuk arkitektur sistem dengan kemudahan kelewahan yang bersesuaian. Perkara yang perlu diambil kira adalah seperti berikut: a) Menyediakan ketersediaan kelewahan rangkaian bagi kemudahan operasi ICT; b) Menggalakkan persekitaran pusat data di lokasi berbeza (*mirrored system*); c) Menggunakan sumber punca kuasa elektrik secara duplikasi; d) Menggunakan perkakasan atau perisian yang mempunyai fungsi *automatic load balancing*; dan e) Mempunyai komponen pendua dalam perkakasan pelayan atau rangkaian.	i. Pengurus ICT ii. ICTSO iii. Pentadbir Pusat Data iv. Pentadbir Rangkaian ICT

KAWALAN 8.15 - *LOGGING*

Objektif : Semua aktiviti dan bukti kewujudan insiden hendaklah direkodkan untuk tujuan jejak audit.

8.15.1 Polisi Log Aktiviti	**Tanggungjawab**
Aktiviti log perlu mengandungi perkara seperti berikut: a) ID pengguna; b) Aktiviti sistem; c) Tarikh, masa dan butiran aktiviti yang dilakukan; d) Percubaan gagal dan berjaya akses masuk ke sistem; e) Percubaan gagal dan berjaya akses maklumat; f) Perubahan konfigurasi sistem; g) Merekodkan kan aktiviti pentadbiran dan operator sistem; dan	i. ICTSO ii. Pentadbir Rangkaian ICT iii. Pentadbir Sistem iv. Pengurus Projek

h) Menyimpan log audit untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	
8.15.2 Kawalan Perlindungan Log	**Tanggungjawab**
Semua pengguna yang mempunyai akses tidak dibenarkan memadam atau menyahaktifkan rekod log. Kawalan perlindungan ke atas rekod log bertujuan untuk melindungi daripada perubahan yang tidak dibenarkan ke atas rekod log seperti berikut: a) Merekodkan perubahan yang dilakukan; b) Fail log yang diubah atau dihapus; c) Kegagalan merekodkan aktiviti rekod lama sekiranya media storan yang menyimpan log telah penuh; d) Melindungi maklumat log daripada capaian yang tidak dibenarkan; e) Capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja; f) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; g) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CDO; h) Merekodkan dan mengambil tindakan ke atas kesalahan, kesilapan dan/ atau penyalahgunaan log; dan i) Memastikan masa (*time stamp*) dalam sistem aplikasi diselaraskan dengan waktu rekod log.	i. ICTSO ii. Pentadbir Rangkaian ICT iii. Pentadbir Sistem iv. Pengurus Projek
8.15.3 Analisis Log	**Tanggungjawab**
Rekod log perlu dianalisis untuk mengenal pasti aktiviti yang boleh menyebabkan sistem aplikasi diceroboh oleh	i. ICTSO ii. Pentadbir

pihak yang tidak dibenarkan. Aktiviti analisis log perlu mengandungi perkara berikut: a) Melaksanakan analisis log; b) Merekodkan kan maklumat bagi setiap insiden atau kejadian keselamatan; c) Pengecualian yang dibenarkan telah dikenal pasti dalam polisi; d) Keputusan hasil analisis; e) Menyemak percubaan yang berjaya atau gagal kepada kemudahan ICT; f) Memantau rekod log fizikal; dan g) Menyemak dan menyelaras kesemua log fizikal untuk mendapatkan analisis yang lebih tepat.	Sistem iii. Pengurus Projek
8.15.4 Log Pentadbir dan Pengendali (*Operator*)	**Tanggungjawab**
Semua log aktiviti pentadbir dan pengendali sistem direkodkan dan log hendaklah dilindungi serta disemak secara berkala. Perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh sekurangkurangnya satu tahun atau tempoh yang dipersetujui bagi membantu mengenal pasti kejadian insiden keselamatan; dan b) Sekiranya wujud aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada CSIRT.	i. ICTSO ii. Pentadbir Sistem iii. Pengurus Projek
KAWALAN 8.16 – AKTIVITI PEMANTAUAN (*MONITORING ACTIVITIES*)	
Objektif: Memastikan insiden keselamatan maklumat dapat dikesan dan pemantauan dilaksanakan secara berkala.	
8.16.1 Aspek Pemantauan	**Tanggungjawab**

Tahap pemantauan perlu ditetapkan mengikut keperluan keselamatan maklumat berdasarkan kepada peraturan dan undang-undang semasa yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Trafik keluar masuk rangkaian dan sistem aplikasi; b) Akses ke sistem, pelayan, peranti rangkaian dan sebagainya; c) Fail konfigurasi bagi semua aplikasi dan peralatan kritikal; d) Log daripada peranti keselamatan; e) Log aktiviti sistem aplikasi dan rangkaian; f) Memastikan kod sumber yang sahih digunakan dan tidak diubahsuai; dan g) Penggunaan dan keupayaan sumber seperti *CPU, memory*, dan *bandwidth*.	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem iv. CSIRT
8.16.2 Pemantauan Aktiviti Anomali	**Tanggungjawab**
Perkara yang perlu dipantau adalah seperti berikut: a) Proses yang ditamatkan tanpa kebenaran; b) Trafik aktiviti yang mengandungi perisian hasad atau meragukan daripada alamat domain atau *IP Address* yang telah dikenal pasti terjejas; c) Ciri-ciri serangan yang dikenal pasti seperti DDOS; d) Aktiviti sistem yang luar biasa seperti *process injection*; e) Proses yang melebihi kebiasaan dan menyebabkan kesesakan trafik; f) Akses yang tidak dibenarkan ke atas sistem; g) Pengimbasan tanpa kebenaran ke atas sistem dan rangkaian; h) Cubaan akses sama ada berjaya atau tidak kepada kemudahan ICT yang dilindungi seperti pelayan DNS;	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem iv. CSIRT

i) Aktiviti pengguna atau sistem yang luar biasa daripada kebiasaan; dan j) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*), kehilangan fizikal (*physical loss*) dan lain-lain yang berkaitan.	
8.16.3 Kawalan Pemantauan Aktiviti Anomali	**Tanggungjawab**
Perkara yang perlu dipantau adalah seperti berikut: a) Memanfaatkan atau menggunakan sistem *threat intelligence;* b) Memastikan keupayaan bagi teknik pembelajaran mesin (*machine learning*) dan *threat intelligence*; c) Menggunakan kaedah senarai yang disekat atau dibenarkan; d) Menggunakan penilaian teknikal keselamatan untuk mengenal pasti garis panduan ciri keselamatan yang dibenarkan; e) Menggunakan sistem pemantauan keupayaan untuk mengesan trafik yang meragukan; dan f) Menggunakan sistem log untuk tujuan pemantauan.	i. Pengurus ICT ii. ICTSO iii. Pentadbir Sistem iv. CSIRT
KAWALAN 8.17 – PENYERAGAMAN WAKTU (*CLOCK SYNCHRONIZATION*)	
Objektif : Memastikan analisis berkaitan aktiviti keselamatan serta data lain yang direkodkan selari dengan Waktu Piawai Malaysia (MST).	
8.17.1 Penyeragaman Waktu	**Tanggungjawab**
Memastikan waktu bagi sistem pemprosesan maklumat atau peralatan hendaklah diselaraskan dengan Waktu Piawai Malaysia (MST). Penyeragaman waktu bagi perkhidmatan awan hendaklah mengikut penyedia perkhidmatan awan (CSP) dan perbezaannya perlu dipantau dan direkodkan untuk mengurangkan risiko percanggahan	i. ICTSO ii. Pentadbir Pusat Data iii. Pengurus Projek iv. Bahagian Keselamatan

KAWALAN 8.18 – PENGGUNAAN PROGRAM UTILITI KHAS (*USE OF PRIVILEGED UTILITY PROGRAMS*)	
Objektif: Memastikan penggunaan program utiliti tidak menjejaskan kawalan sistem dan aplikasi bagi keselamatan maklumat.	
8.18.1 Penggunaan Program Utiliti	**Tanggungjawab**
Penggunaan sistem utiliti (contoh: *wireshark, putty, ip scanner* dan lain-lain) perlulah dikawal dan dihadkan kepada pegawai yang dibenarkan saja. Panduan seperti di bawah perlu dipatuhi: a) Mengehadkan bilangan pengguna yang dibenarkan untuk menggunakan program utiliti; b) Memastikan penggunaan ID yang unik untuk pengesahan dan kebenaran akses; c) Mengenal pasti dan mendokumenkan program utility yang diberikan kebenaran; d) Membenarkan penggunaan program utiliti pada waktu luar jangka *(ad-hoc)*; e) Menghapuskan dan menutup program utiliti yang tidak berkaitan; f) Mengehadkan ketersediaan program utiliti; g) Menyimpan log program utiliti; dan h) Penggunaan program utiliti yang membebankan kapasiti (*bandwidth*) rangkaian perlu dihadkan.	i. ICTSO ii. Pentadbir Sistem

KAWALAN 8.19 – PEMASANGAN PERISIAN PADA SISTEM PENGOPERASIAN (*INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS*)	
Objektif : Memastikan penggunaan perisian yang dibenarkan pada peralatan ICT.	
8.19.1 Kawalan Pemasangan Perisian	**Tanggungjawab**
Perkara berikut perlu dipatuhi bagi sebarang pemasangan atau perubahan perisian: a) Pengemaskinian versi sistem pengoperasian hanya boleh dilakukan oleh Pentadbir ICT;	Semua

b) Memastikan hanya "*executable code*" yang diluluskan digunakan dalam sistem operasi; c) Memasang dan mengemas kini perisian yang telah diuji keberkesanan sahaja; d) Memastikan semua sumber *libraries* program yang terkini; e) Menggunakan sistem pengurusan konfigurasi untuk mengawal konfigurasi dan dokumentasi sistem; f) Menetapkan strategi pembentukan semula (*rollback*) sebelum perubahan dilaksanakan dan melaksanakan jika perlu; g) Memastikan log audit direkodkan bagi semua pengemaskinian; h) Memastikan versi lama perisian diarkibkan dan direkodkan untuk kegunaan memproses data sekiranya diperlukan; i) Hanya perisian yang dibenarkan bagi kegunaan di jabatan; j) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana peraturan dan undang-undang semasa yang berkuat kuasa; k) Mengimbas semua perisian atau sistem dengan *endpoint security* sebelum menggunakannya; dan l) Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.	
KAWALAN 8.20 – KESELAMATAN RANGKAIAN	
Objektif: Memastikan pengurusan keselamatan perkhidmatan rangkaian dilaksanakan bagi melindungi maklumat dan kemudahan ICT daripada ancaman dalaman dan luaran.	
8.20.1 Kawalan Infrastruktur Rangkaian	**Tanggungjawab**

Infrastruktur rangkaian hendaklah dirancang, diurus dan dikawal bagi melindungi keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah: a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat dan pengoperasian infrastruktur rangkaian; b) Memastikan pengemaskinian maklumat rangkaian secara berterusan seperti diagram rangkaian dan fail konfigurasi infrastruktur rangkaian; c) Peralatan keselamatan seperti *firewall* hendaklah dipasang bagi memastikan kawalan capaian kepada infrastruktur ICT jabatan dapat dilaksanakan; d) Memantau cubaan pencerobohan dan aktiviti yang boleh mengancam sistem dan maklumat jabatan melalui pemasangan peralatan keselamatan seperti *Intrusion Prevention System (IPS), Intrusion Detection System (IDS) dan Web Application Firewall (WAF)*; e) Peralatan rangkaian hendaklah diletakkan di lokasi yang bebas dari risiko seperti banjir, gegaran dan habuk; f) Sebarang keperluan penyambungan rangkaian hendaklah melalui proses dan prosedur yang ditetapkan; g) Penggunaan rangkaian tanpa wayar *(wireless)* LAN di jabatan hendaklah mematuhi peraturan yang dikeluarkan oleh pihak berkenaan seperti Jabatan Digital Negara (JDN) dan Majlis Keselamatan Negara (MKN); h) Semua perisian berkaitan rangkaian dan keselamatan seperti *sniffer atau network analyzer* adalah dilarang dipasang kecuali mendapat kebenaran ICTSO; dan h) Memastikan kawalan keselamatan yang sesuai untuk penggunaan rangkaian maya seperti *Virtual Private*	i. ICTSO ii. Pentadbir Rangkaian iii. Pihak Ketiga

Network (VPN) dan *Zero Trust Network Access* (ZTNA).	

KAWALAN 8.21 – KESELAMATAN PERKHIDMATAN RANGKAIAN

Objektif: Memastikan kaedah keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian dikenal pasti, dilaksana dan dipantau.

8.21.1 Keselamatan Perkhidmatan Rangkaian	**Tanggungjawab**
Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi menjamin kerahsiaan, integriti dan ketersediaan maklumat. Perkara-perkara yang perlu dipatuhi adalah: a) Mekanisma keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara dalaman atau menggunakan sumber luar; b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalan jabatan; c) Sebarang aktiviti yang dilarang seperti yang digariskan dalam Peraturan/ Pekeliling semasa yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering;* dan d) Mempunyai kawalan akses kepada perkhidmatan rangkaian yang disediakan mengikut peranan yang diluluskan.	i. ICTSO ii. Pentadbir Rangkaian iii. Penyedia Perkhidmatan Rangkaian iv. Pihak Ketiga

KAWALAN 8.22 – PENGASINGAN RANGKAIAN

Objektif: Memastikan pengasingan kawalan sempadan ke atas perkhidmatan rangkaian yang disediakan untuk meminimumkan risiko ancaman atau pengubahsuaian yang tidak dibenarkan.

8.22.1 Pengasingan Rangkaian	**Tanggungjawab**

Pengasingan perkhidmatan rangkaian bertujuan untuk meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: a) Mengenal pasti fungsi dan tanggungjawab pengguna; b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Mengemas kini hak capaian pengguna dari semasa ke semasa mengikut keperluan; dan e) Operasi rangkaian hendaklah diasing bagi meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	i. ICTSO ii. Pentadbir Rangkaian iii. Pihak Ketiga

KAWALAN 8.23 – PENAPISAN WEB

Objektif: Memastikan akses ke laman web dilindungi dan menyekat akses ke laman web yang tidak dibenarkan.

8.23.1 Tapisan Web	**Tanggungjawab**
Kawalan penyaringan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat akses ke laman web yang dianggap tidak selamat dan tidak produktif bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan. Perkara-perkara yang perlu dipatuhi adalah: a) Menyekat alamat IP atau domain laman web yang tidak sah; b) Menyekat laman web berbahaya seperti *phishing* dan *malicious* berdasarkan fungsi *threat intelligence* dalam peralatan keselamatan web; dan	i. ICTSO ii. Pentadbir Rangkaian iii. Pihak Ketiga

Mengemaskini pangkalan data ancaman (*signature database*) dalam peralatan keselamatan web melalui sumber yang sahih.	

KAWALAN 8.24 – PENGGUNAAN KRIPTOGRAFI

Objektif: Memastikan penggunaan kriptografi untuk melindungi kerahsiaan dan integriti maklumat berdasarkan keperluan jabatan dengan mematuhi keperluan Peraturan/ Pekeliling semasa yang berkuat kuasa.

8.24.1 Kriptografi	**Tanggungjawab**
Kriptografi bermaksud teknik penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja. Tindakan melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi yang boleh dilakukan adalah seperti berikut: a) Penggunaan enkripsi, fungsi *hash* dan *Message Authentication Code* (MAC) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; b) Penggunaan tanda tangan digital digalakkan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik; c) Pengurusan ke atas *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut; d) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan e) Kawalan ke atas kemudahan had capaian maklumat.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

KAWALAN 8.25 – KITARAN HAYAT PEMBANGUNAN YANG SELAMAT	
Objektif: Memastikan pembangunan sistem aplikasi menggunakan persekitaran yang selamat sepanjang tempoh pembangunan sistem.	
8.25.1 Persekitaran Pembangunan Sistem yang Selamat	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Aspek keselamatan pembangunan perlu diambil kira dalam perkhidmatan, infrastruktur, perisian dan sistem. b) Mengasingkan persekitaran sebenar (*production*), pembangunan dan pengujian; c) Keperluan keselamatan dalam fasa spesifikasi, reka bentuk pengurusan projek; d) Pengujian keselamatan seperti ujian penembusan, semakan kod pengaturcaraan dan pengujian pepijat (*bugs*) kod pengaturcaraan selepas pengemaskinian; e) Penyimpanan kod sumber dan konfigurasi sistem aplikasi di tempat yang selamat; f) Memastikan kawalan keselamatan ke atas perubahan versi sistem aplikasi; g) Menyediakan keperluan latihan keselamatan sistem aplikasi untuk meningkatkan kemahiran teknikal pembangun sistem bagi mengenal pasti dan menyelesaikan kelemahan ke atas aplikasi; h) Memastikan keperluan lesen diambil kira atau dan menggunakan alternatif lain bagi kawalan kos yang efektif; dan i) Memastikan pembangunan yang dilaksanakan oleh pihak ketiga mengambil kira kitar hayat pembangunan secara selamat dalam kontrak perjanjian.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

KAWALAN 8.26 – KEPERLUAN KESELAMATAN APLIKASI	
Objektif: Memastikan semua keperluan keselamatan maklumat dikenal pasti dan dilaksanakan semasa pembangunan atau penambahbaikan sistem aplikasi.	
8.26.1 Keperluan Keselamatan Aplikasi	**Tanggungjawab**
Maklumat aplikasi hendaklah dilindungi daripada aktiviti tidak sah seperti penipuan, pendedahan maklumat dan pengubahsuaian maklumat yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: a) Memastikan pengguna mempunyai tahap akses yang dibenarkan; b) Mengenal pasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi; c) Membezakan had akses kepada data dan fungsi dalam sistem aplikasi; d) Ketahanan terhadap ancaman perisian hasad atau gangguan pihak yang tidak dibenarkan; e) Memastikan perundangan dan peraturan dipatuhi bagi transaksi yang dijana, diproses, dilengkapkan atau disimpan; f) Memastikan maklumat rahsia rasmi dilindungi; g) Memastikan data yang diproses dan dipindahkan dilindungi; h) Memastikan komunikasi antara semua pihak dienkripsi dengan selamat; i) Melaksanakan pengesahan input; j) Mengawal kelulusan yang dijana oleh Sistem Aplikasi seperti mengehadkan kelulusan atau kelulusan melebihi satu orang pelulus;	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pengguna vi. Pihak Ketiga

k) Mengawal kebenaran untuk akses kepada output yang dihasilkan; l) Mengehadkan kandungan medan *free text* bagi mengawal kapasiti storan; m) Melaksanakan pemantauan dan Merekodkan kan log transaksi ke atas proses kerja; n) Memastikan kawalan keselamatan sistem aplikasi seperti penggunaan perisian log atau sistem pengesanan kebocoran data; dan o) Pengendalian mesej ralat.	
8.26.2 Transaksi Perkhidmatan Dalam Talian	**Tanggungjawab**
Perkara-perkara berikut perlu dipatuhi: a) Memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem; b) Memastikan penggunaan kaedah seperti *digital signature, hashing* dan lain-lain untuk mengesahkan identiti penghantar dan penerima semasa pertukaran data; c) Memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi; d) Memastikan semua pihak memahami aspek kerahsiaan, integriti, serta bukti penghantaran dan penerimaan dokumen; e) Memastikan perkhidmatan sistem aplikasi menggunakan *Secure Socket Layer (SSL)* dalam setiap transaksi; f) Menetapkan tempoh transaksi yang disimpan; dan Keperluan kontrak perjanjian.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pengguna vi. Pihak Ketiga

8.26.3 Aplikasi Pesanan dan Pembayaran Elektronik	Tanggungjawab
Sebarang pembangunan sistem yang melibatkan proses bayaran secara dalam talian, perlu merujuk kepada **Surat Pekeliling Akauntan Negara Malaysia (SPANM) Bilangan 4 2018** "Garis Panduan Permohonan Pembangunan Sistem Perakaunan Kewangan Agensi Kerajaan".	i. ICTSO ii. Pengurus iii. Projek Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pengguna vi. Pihak Ketiga

KAWALAN 8.27 – PRINSIP KEJURUTERAAN DAN ARKITE SISTEM YANG SELAMAT

Objektif: Prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumenkan, dikaji dan diguna pakai ke atas semua pembangunan sistem aplikasi berdasarkan Peraturan/ Pekeliling semasa yang berkuat kuasa.

8.27.1 Kriteria Kejuruteraan Sistem Yang Selamat	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: a) Menyediakan kawalan keselamatan untuk melindungi maklumat dan sistem aplikasi daripada ancaman yang dikenal pasti; b) Mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan; c) Memastikan semua maklumat rahsia rasmi dienkripsi (*encryption*); d) Mengenal pasti keperluan kawalan keselamatan yang akan dilaksanakan; e) Melaksanakan kawalan keselamatan terhadap individu yang berkaitan;	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

f) Memastikan reka bentuk yang selamat (*secure architecture*) diguna pakai dalam prinsip kejuruteraan dan arkitektur sistem; g) Memastikan kawalan keselamatan infrastruktur dilaksanakan seperti penggunaan *Public Key Infrastructure* (PKI), *Identity* and *Access Management* (IAM), pencegahan kebocoran data dan pengurusan akses dinamik; h) Mempunyai kepakaran untuk membangun dan menyelenggara sistem aplikasi selari dengan teknologi yang dipilih atau digunakan; i) Mengambil kira keperluan kos, masa dan cabaran dalam memenuhi keperluan keselamatan; j) Mengguna pakai konsep amalan terbaik (*best practise*); dan k) Melaksanakan *Security Posture Assessment* (SPA) dan *hardening* ke atas sistem aplikasi.	
8.27.2 Prinsip "Zero Trust"	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian; b) Menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi; c) Memastikan sistem aplikasi menggunakan fungsi enkripsi; d) Menyemak dan mengesahkan semua permohonan akses yang diterima; e) Memberikan kategori akses paling minimum kepada pengguna; dan	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

g) Menggunakan pengesahan keselamatan ketika log masuk atau transaksi yang melibatkan sistem aplikasi seperti captcha, security phrase dan secure transaction authorisation code (TAC)	

KAWALAN 8.28 – PENGEKODAN SELAMAT

Objektif: Memastikan penggunaan kod pengaturcaraan yang selamat bagi meminimumkan kelemahan (*vulnerabilities*) dalam sistem aplikasi.

8.28.1 Fasa Perancangan Pengekodan Selamat	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Pembangunan sistem aplikasi sama ada secara dalaman (*inhouse*) atau luaran (*outsource*) hendaklah menggunakan pengekodan selamat berdasarkan kepada peraturan dan keperluan yang dikuatkuasakan; b) Memastikan amalan dan kelemahan pengekodan yang berlaku sebelum ini dijadikan sebagai sumber rujukan supaya kelemahan keselamatan maklumat yang sama tidak berulang; c) Menggalakkan penggunaan perisian Pembangunan seperti *Integrated Development Environments (IDE)* untuk membantu pengekodan selamat; d) Penggunaan persekitaran pembangunan semasa fasa pembangunan sistem aplikasi; e) Memastikan penggunaan perisian pembangunan yang terkini; f) Memastikan pembangun sistem atau pihak ketiga yang dilantik mempunyai kemahiran dalam pembangunan sistem aplikasi menggunakan pengekodan selamat; dan g) Memastikan arkitektur, rekabentuk dan standard pengekodan digunakan dalam persekitaran yang selamat.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

8.28.2 Fasa Semasa Pengekodan Selamat	Tanggungjawab
Perkara yang perlu diambil kira adalah seperti berikut: a) Memastikan penggunaan teknik dan struktur pengekodan selamat bagi bahasa pengaturcaraan yang digunakan seperti *pair programming, refactoring* dan *test-driven development*; b) Merekodkan dan memperbaiki kelemahan kod sumber yang boleh terdedah kepada ancaman daripada dieksploitasi; c) Menggunakan perisian yang terkini dan tidak tamat tempoh *end of support* (EOS); d) Memastikan tidak menggunakan teknik pembangunan yang tidak selamat seperti *hard-coded passwords, unapproved code samples* dan *unauthenticated web services*; e) Melaksanakan pengujian keselamatan maklumat dan tindakan pembaikan. f) Melaksanakan analisa berkaitan kesalahan umum kod pengaturcaraan dan Merekodkan kan tindakan pembetulan.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga
8.28.3 Fasa Penyelenggaraan dan Kajian Semula	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Memastikan *patches* dan *security updates* perisian sentiasa dikemas kini; b) Kelemahan keselamatan maklumat yang dilaporkan hendaklah diambil tindakan; c) Ralat dan cubaan serangan hendaklah direkodkan serta disemak secara berkala bagi penambahbaikan ke atas kod	i. ICTSO ii. Pengurus Projek iii. Pembangun iv. Sistem Aplikasi v. Pentadbir Sistem vi. Pihak Ketiga

pengaturcaraan sekiranya perlu; dan c) Kod sumber hendaklah dilindungi daripada akses dan gangguan yang tidak dibenarkan seperti menggunakan fungsi kawalan versi (*version control*). d) Sekiranya menggunakan *external tools and libraries*, perkara seperti di bawah hendaklah diambil kira: i. *External tools and libraries* yang digunakan adalah versi terkini; atau ii. Komponen seperti pengesahan kriptografi komponen yang telah disahkan dan stabil; iii. Lesen, keselamatan dan komponen luaran yang sah; iv. *External tools and libraries* boleh diselenggara dan diperolehi daripada sumber yang dipercayai; atau v. Ketersediaan sumber yang mencukupi untuk rujukan pembangunan jangka panjang. e) Sekiranya *software package* perlu ditambah baik, perkara seperti di bawah hendaklah diambil kira: i. Risiko kepada fungsi kawalan sedia ada dan integriti perisian tersebut; ii. Perlu mendapatkan kebenaran daripada pemilik perisian; iii. Keperluan untuk menjadikan perubahan tersebut sebagai versi terkini; iv. Kesan kepada jabatan sekiranya dipertanggungjawabkan untuk menyelenggara perubahan perisian tersebut; dan v. Keserasian (*compatibility*) dengan perisian yang lain.	

KAWALAN 8.29 – PENGUJIAN KESELAMATAN SEMASA PEMBANGUNAN DAN PENERIMAAN	
Objektif: Memastikan keperluan keselamatan maklumat dipenuhi semasa sistem aplikasi digunakan dalam persekitaran sebenar.	
8.29.1 Pengujian Keselamatan Sistem Aplikasi	**Tanggungjawab**
Pengujian keselamatan hendaklah merangkumi perkara berikut: a) Fungsi keselamatan bagi sistem aplikasi yang baharu dan dinaik taraf hendaklah diuji semasa fasa Pembangunan seperti pengujian pengesahan pengguna, kawalan akses, penggunaan kriptografi dan pengekodan selamat. b) Konfigurasi keselamatan yang melibatkan sistem pengoperasian, *firewalls* dan komponen keselamatan lain hendaklah diuji; dan c) *Security Posture Assessment* (SPA) hendaklah dilaksanakan ke atas semua sistem aplikasi baharu atau penambahbaikan sistem aplikasi; d) Pelan pengujian penerimaan system hendaklah disediakan dan mengandungi perkara berikut: i. Jadual aktiviti pengujian; ii. Input dan output yang dijangka supaya memenuhi senarai syarat yang telah ditentukan; iii. Kriteria untuk menilai keputusan; iv. Memastikan proses kerja sistem aplikasi memenuhi keperluan pengguna; dan v. keputusan pengujian yang memerlukan tindakan lanjut sekiranya diperlukan. e) Pengujian awal bagi sistem yang dibangunkan secara dalaman hendaklah dilaksanakan oleh pasukan pembangun sistem. Pengujian Penerimaan hendaklah dilaksanakan ke atas semua sistem aplikasi baharu	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

atau penambahbaikan sistem aplikasi oleh pihak ketiga yang tidak terlibat dengan pembangunan sistem. i) Melaksanakan aktiviti semakan kod pengaturcaraan untuk mengenal pasti kelemahan termasuk input dan ralat yang tidak dijangka; ii) Melaksanakan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem aplikasi; iii) Melaksanakan pengujian penembusan (*penetration testing*) untuk mengenal pasti reka bentuk dan kod sumber tidak selamat. f) Bagi pembangunan sistem secara luaran atau pembelian, proses perolehan mestilah dilaksanakan mengikut peraturan/ pekeliling semasa yang berkuat kuasa. g) Penilaian produk dan perkhidmatan hendaklah dilaksanakan sebelum perolehan dilaksanakan; h) Perjanjian bersama pihak ketiga perlu mengandungi keperluan keselamatan; i) Persekitaran pengujian hendaklah sama dengan persekitaran sebenar supaya pengujian tersebut tidak boleh disangkal dan boleh dipercayai.	

KAWALAN 8.30 – PEMBANGUNAN SISTEM SECARA LUARAN	
Objektif: Pembangunan sistem aplikasi yang dilaksanakan oleh pihak ketiga perlu dikawal selia dan dipantau bagi memastikan keselamatan maklumat dipatuhi berdasarkan Peraturan/ Pekeliling semasa yang berkuat kuasa.	
8.30.1 Pembangunan Sistem Secara Luaran	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Memastikan perjanjian lesen, *Intellectual Property Rights* (IPR) dan kod sumber menjadi hak milik kerajaan;	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi

b) Memastikan klausa kontrak mengandungi klausa berhubung keperluan keselamatan reka bentuk, keselamatan pengaturcaraan dan pengujian. c) Melaksanakan pengujian penerimaan untuk memastikan kualiti dan output memenuhi keperluan; d) Memastikan pengujian keselamatan, kelemahan yang dikenal pasti dan tindakan pembetulan dilaksanakan adalah mencukupi sebelum penyerahan projek; e) Memasukkan klausa dalam kontrak yang membenarkan pelaksanaan audit terhadap proses pembangunan dan kod sumber; dan f) Keperluan keselamatan untuk persekitaran pembangunan. g) Mempertimbangkan sebarang perundangan yang berkuat kuasa seperti Akta Perlindungan Data Peribadi.	iv. Pentadbir Sistem v. Pihak Ketiga
KAWALAN 8.31 – PENGASINGAN PERSEKITARAN PEMBANGUNAN (*DEVELOPMENT*), PERSEKITARAN PENGUJIAN (*TESTING*) DAN PERSEKITARAN SEBENAR (*PRODUCTION*)	
Objektif: Memastikan keselamatan maklumat dalam semua persekitaran ICT dilindungi daripada ancaman oleh pihak tidak dibenarkan.	
8.31.1 Pengasingan Persekitaran Pembangunan (*Development*), Persekitaran Pengujian (*Testing*) dan Persekitaran Sebenar (*Production*)	**Tanggungjawab**
Perkara yang perlu diambil kira adalah seperti berikut: a) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan sebenar; b) Merekodkan semua penggunaan sumber yang dilaksanakan; c) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti;	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga

d) Mengasingkan persekitaran sebenar dengan pembangunan dalam segmen rangkaian dan infrastruktur yang berbeza; e) Menetapkan, Merekodkan kan dan melaksanakan peraturan serta pengesahan untuk penggunaan sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran sebenar; f) Melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam persekitaran sebenar; g) Memastikan *compilers*, *editor* dan *tools* pembangunan atau program utiliti lain tidak dipasang di persekitaran sebenar; h) Tidak menggunakan maklumat sebenar pada persekitaran pembangunan atau persekitaran pengujian kecuali dengan kawalan keselamatan; i) Mengemaskini *patches*, pembangunan sistem aplikasi, integrasi dan tools pengujian seperti *builders*, *integrators*, *compilers*, sistem konfigurasi dan *libraries*; j) Memantau dan memastikan kawalan akses persekitaran; dan k) Menyediakan sandaran (*backup*) mengikut persekitaran.	
KAWALAN 8.32 – PENGURUSAN PERUBAHAN	
Objektif : Memastikan pengurusan perubahan dalam persekitaran ICT dilaksanakan dengan mengambil kira kawalan keselamatan maklumat.	
8.32.1 Prosedur Kawalan Perubahan	**Tanggungjawab**
Prosedur kawalan perubahan perlu mengambil kira perkara berikut:	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi

a) Perubahan yang dilaksanakan telah mendapat kelulusan; b) Perubahan yang dilaksanakan dimaklumkan kepada pihak berkepentingan; c) Melaksanakan pengujian penerimaan terhadap perubahan; d) Perubahan ke atas perkakasan, perisian atau sistem aplikasi mengambil kira aspek keselamatan maklumat; e) Perubahan ke atas perkakasan, perisian atau sistem aplikasi ini hanya dilaksanakan oleh pihak yang dibenarkan sahaja; f) Perubahan atau pengubahsuaian ke atas perkakasan, perisian atau sistem aplikasi hendaklah diuji, direkodkan dan disahkan sebelum diguna pakai; g) Pelan pelaksanaan perubahan seperti pembangunan, pengujian dan *deployment*; h) Memastikan prosedur pembentukan semula (*fallback*) dilaksanakan sebagai pelan perancangan luar jangka (*contingency*); i) Merekodkan kan semua perubahan yang dilaksanakan; j) Memastikan manual operasi pengguna dan sistem aplikasi diubah mengikut keperluan; k) Memastikan prosedur pelan kesinambungan perkhidmatan dan pemulihan ICT diubah mengikut keperluan; l) Setiap perubahan kepada pengoperasian sistem perlu dikaji dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap keselamatan maklumat; m) Perubahan kepada kod pengaturcaraan (*source code*) sistem aplikasi perlu dihadkan kepada pengguna yang dibenarkan; dan	iv. Pentadbir Sistem v. Pihak Ketiga vi. Pengguna

n) Memastikan perubahan ke atas perkakasan, perisian atau sistem aplikasi tidak menjejaskan perkhidmatan operasi sistem maklumat. o) Sebarang kerja pengubahsuaian atau naik taraf peranti rangkaian perlulah mendapat kelulusan Pengurus ICT dan diselia oleh Pentadbir Rangkaian;	

KAWALAN 8.33 – DATA PENGUJIAN

Objektif: Memastikan data yang digunakan semasa pengujian dilindungi dan dikawal mengikut peraturan yang ditetapkan.

8.33.1 Penggunaan Data	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Identiti penguji perlu dikenal pasti dan disahkan bagi menentukan tahap capaian maklumat yang dibenarkan; b) Setiap penguji sistem perlu diberi peranan mengikut skop dan tanggungjawab yang ditetapkan; c) Melaksanakan kawalan akses yang sama di persekitaran sebenar dan persekitaran pengujian; d) Menyediakan hak akses berlainan setiap kali maklumat digunakan ke persekitaran pengujian; e) Menyimpan log penyalinan dan penggunaan maklumat operasi bagi tujuan jejak audit; f) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; g) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; dan h) Melindungi maklumat rahsia rasmi dengan menghapus data setelah pengujian selesai.	i. ICTSO ii. Pengurus Projek iii. Pembangun Sistem Aplikasi iv. Pentadbir Sistem v. Pihak Ketiga vi. Pengguna

KAWALAN 8.34 – PERLINDUNGAN SISTEM MAKLUMAT SEMASA UJIAN AUDIT

Objektif: Memastikan penilaian pengujian audit dilaksanakan ke atas proses kerja sistem aplikasi.

8.34.1 Pengauditan	Tanggungjawab
Perkara yang perlu dipatuhi adalah seperti berikut: a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; b) Mendapatkan kebenaran untuk melaksanakan ujian audit berdasarkan kawalan dan skop yang dibenarkan; c) Capaian ke atas sistem maklumat semasa pengauditan perlu dikawal selia bagi mengelakkan sebarang penyalahgunaan. d) Mendapatkan kebenaran untuk capaian kepada sistem aplikasi dan data bagi ujian audit; e) Memastikan data yang dibenarkan hanya berstatus *Read Only* semasa ujian audit dilaksanakan; f) Jika terdapat keperluan capaian lebih daripada *Read Only*, pengujian hendaklah dilaksanakan oleh pentadbir yang dibenarkan bagi membantu juru audit; g) Memastikan keperluan keselamatan perkakasan juru audit dipatuhi seperti penggunaan antivirus sebelum kebenaran diberikan; h) Membenarkan capaian kepada sistem fail oleh juru audit dan menghapuskan data tersebut setelah audit selesai atau melaksanakan kawalan keselamatan yang bersesuaian; i) Memastikan penggunaan peralatan audit (*audit tools*) mendapat kelulusan terlebih dahulu; j) Melaksanakan ujian audit di luar waktu bekerja sekiranya menyebabkan gangguan perkhidmatan; dan k) Menyimpan dan memantau semua akses semasa ujian audit.	i. ICTSO ii. Pasukan ISMS INSTUN iii. Pentadbir Sistem Aplikasi

SENARAI LAMPIRAN

KAKITANGAN JABATAN - LAMPIRAN A (I)

PEMBEKAL/ PIHAK KETIGA - LAMPIRAN A (I), B (I) & B (II)

LAMPIRAN A (I)

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
INSTITUT TANAH DAN UKUR NEGARA (INSTUN)

Nama (HURUF BESAR) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber; dan

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Tandatangan & Cap Jawatan)

Institut Tanah dan Ukur Negara

Tarikh: .....

* Polisi Keselamatan Siber boleh dicapai menerusi https://www.instun.gov.my

.....

LAMPIRAN B (I)

PERAKUAN UNTUK DITANDATANGANI OLEH 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*]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukanperuntukan Akta Rahsia Rasmi 1972 [*Akta 88*] dan bahawa 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 rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu 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.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh 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, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan 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 : .....

Cap Jabatan / Organisasi : .....

.....

LAMPIRAN B (II)

PERAKUAN UNTUK DITANDATANGANI OLEH 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*]

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 rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu 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 dengan 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 Baginda 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 : .....

Cap Jabatan / Organisasi : .....

RUJUKAN

SENARAI PERUNDANGAN DAN PERATURAN

1. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 bertajuk "Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
2. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam – 1 Ogos 2022.
3. Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022
4. Pekeliling Bilangan 8 Tahun 2024 - Garis Panduan Pengurusan Dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam";
5. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam";
6. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam";
7. Arahan Keselamatan (Semakan dan Pindaan 2017).
8. Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.
9. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002.
10. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan.
11. 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.
12. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007.
13. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.
14. Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan.
15. Akta Keselamatan Siber 2024 (Act 854)

16. Akta Tandatangan Digital 1997.
17. Akta Rahsia Rasmi 1972.
18. Akta Jenayah Komputer 1997.
19. Akta Hak Cipta (Pindaan) Tahun 1997.
20. Akta Komunikasi dan Multimedia 1998.
21. Perintah - Perintah Am.
22. Arahan Perbendaharaan.
23. Arahan Teknologi Maklumat 2007.
24. Garis Panduan Keselamatan MAMPU 2004.
25. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009.
26. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan.
27. Arahan Teknologi Maklumat dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007).
28. Pekeliling Am Bil. 1 Tahun 2009 – Manual Pengurusan Aset Menyeluruh Kerajaan.
29. Surat Pekeliling Am Bilangan 1 Tahun 2009 Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan.
30. Surat Arahan Ketua Setiausaha Negara – Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain-lain Peralatan Komunikasi ICT Tanpa Kebenaran (Tarikh : 31 Januari 2007).
31. Surat Arahan Ketua Pengarah MAMPU – Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh : 8 April 2011).
32. Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan Dan Pengurusan E-Mel (Tarikh : 1 Julai 2010).
33. Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam (5 Mac 2010).
34. Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam (Tarikh : 4 Januari 2010).
35. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial Di Sektor Awam (Tarikh : 19 November 2009).
36. Surat Arahan Ketua Pengarah MAMPU – Penggunaan Smartphone, Personel Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh : 15 September 2009).
37. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010).

38. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007).
39. Garis Panduan IT Outsourcing (Oktober 2006).
40. Garis Panduan Penyimpanan dan Pe-meliharaan Rekod Elektronik Sektor Awam.
41. Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.
42. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
43. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.
44. Rancangan Malaysia Ke-11.
45. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.
46. Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
47. Dasar Kriptografi Negara 12 Julai 2013.
48. Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013.
49. Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.
50. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
51. Arahan Ketua Pegawai Keselamatan Kerajaan 5 Jun 2012 – Langkah-langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam.
52. PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).
53. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 November 2010.
54. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Januari 2010.
55. Akta 709 – Akta Perlindungan Data Peribadi 2010.
56. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan, 23 November 2007.
57. Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lainlain Peralatan Komunikasi ICT Tanpa Kebenaran Atau Kuasa Yang Sah Di Agensiagensi Kerajaan.
58. Surat Arahan Ketua Setiausaha Negara - Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-agensi Kerajaan, 20 Oktober 2006.

59. Akta 658 – Akta Perdagangan Elektronik 2006.
60. Akta 629 – Akta Arkib Negara 2003.
61. Akta 606 – Akta Cakera Optik 2000.
62. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).
63. Akta 56 – Akta Keterangan 1950.
64. National Cyber Security Policy (NCSP).
65. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/ Organisations.
66. Arahan Tetap Sasaran Penting.
67. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
68. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
69. Perintah Am Bab D.
70. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016.
71. ISO/IEC 27001:2022