PENGURUSAN PENGENDALIAN INSIDEN
KESELAMATAN TEKNOLOGI MAKLUMAT DAN
KOMUNIKASI (ICT) SEKTOR AWAM

POLISI KESELAMATAN SIBER

KEMENTERIAN DALAM NEGERI

KDN-BPTM-PKS

VERSI 1.1

REKOD PINDAAN DOKUMEN

TARIKH	VERSI	MUKA SURAT	BUTIRAN PINDAAN
22/08/2022	1.0	-	Dokumen asal
12/09/2023	1.1	58	Pengurusan Keselamatan Konfigurasi • Objektif • Keselamatan Konfigurasi
		59	*Data Leakage Prevention* (DLP) • Objektif • Pencegahan Kebocoran Data
		90	Penambahan rujukan dan Senarai Perundangan 1. Garis Panduan Penkomputeran Awan 2. Pekeliling Perkhidmatan Sumber Manusia versi 1.0 (2022)

KANDUNGAN

2 TERMA DAN TAKRIFAN

Antivirus	Perisian yang mengimbas virus pada media storan.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab KDN.
Beyond Economic Repair (BER)	Aset ICT yang tidak lagi optimum dari segi komersil untuk dibaik pulih.
CDO	C*hief Digital Officer* - TKSU Pengurusan atau pegawai yang dilantik oleh KSU
CSIRT	*Computer Security Incident Response*
Denial of Service (DoS)	Halangan pemberian perkhidmatan.
Dokumen	Dokumen digital / fizikal yang berkaitan dengan operasi ICT serta Aset ICT KDN.
DLP	*Data Leakage Prevention* – Pecengahan keselamatan yang membantu menghalang perkongsian , pemindahan atau penggunaan data sensitif yang tidak selamat atau tidak sesuai.
End of Life (EOL)	Aset ICT atau komponen berkaitan yang telah tamat kitaran hidup.
End of Support (EOS)	Aset ICT atau komponen berkaitan tidak lagi diberi sokongan teknikal oleh pembuat Aset tersebut.
Enkripsi	Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

Firewall	Sistem yang direka bentuk untuk mengawal capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
ICTSO	*ICT Security Officer* – Timbalan SUB IT atau pegawai yang dilantik oleh KSU
Jalur lebar	Jalur saluran penghantaran data berkapasiti tinggi.
Local Area Network (LAN)	Rangkaian Kawasan Setempat yang menghubungkan komputer.
Malicious code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus, trojan horse, worm, spyware* dan sebagainya.
MFA	*Multiple-factor Authentication* – Kaedah pengesahan yang memerlukan pengguna menyediakan dua faktor atau lebih faktor pengesahan untuk mendapatkan akses.
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.
NACSA	*National Cyber Security Agency* atau Agensi Keselamatan Siber Negara
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

Pasukan Pemulihan Bencana KDN	Pasukan yang dilantik oleh CDO untuk melaksanakan serta menjalankan pelan bencana.
Pegawai Keselamatan	Wakil CGSO dan PDRM yang berkhidmat di Bahagian Khidmat Pengurusan.
Pegawai Pengelas	Bertanggungjawab menguruskan dokumen rahsia rasmi Kerajaan dari segi pendaftaran, pengelasan, pengelasan semula dan pelupusan serta mematuhi peraturan yang sedang berkuat kuasa.
Pelanggan	Pihak luaran, individu atau syarikat yang menerima perkhidmatan dari KDN.
Pelawat	Individu luar yang dibenarkan untuk melawat premis KDN secara fizikal.
Pembekal	Pihak luaran yang membekalkan perkhidmatan kepada KDN.
Pemilik Projek	Pasukan kerja yang dilantik oleh JPICT bagi memastikan projek dilaksanakan secara sempurna.
Pengguna	Warga KDN dan/atau Pihak Ketiga yang mempunyai akses kepada sistem dan / atau maklumat KDN.
Pengurus ICT	SUB IT BPTM atau pegawai yang dilantik oleh KSU.
Pentadbir ICT	Pegawai yang ditugaskan untuk mentadbir perkakasan dan perisian ICT termasuk sistem pengoperasian, pangkalan data, aplikasi serta rangkaian.
Pihak Ketiga	Pembekal dan Pelanggan KDN.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Risiko	Situasi yang boleh membawa padah atau akibat buruk.

Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, Internet.
Threat	Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan kemusnahan atau musibah.
Uninterruptible Power Supply (UPS)	Perkakasan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Warga KDN	Kakitangan kerajaan yang berkhidmat di Kementerian Dalam Negeri sama ada berjawatan tetap, kontrak dan sambilan yang menggunakan perkhidmatan KDN.
Vulnerablity	Keadaan yang boleh membawa kepada diserang atau dicederakan.

3 PENGENALAN

Polisi Keselamatan Siber (PKS) Kementerian Dalam Negeri (KDN) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) KDN.

Dokumen ini berhubungkait dengan pelaksanaan pengurusan sistem keselamatan maklumat berlandaskan piawaian ISO/IEC 27001:2022.

Dokumen ini juga menerangkan kepada semua pengguna di KDN mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KDN.

4 OBJEKTIF

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

Objektif utama PKS KDN adalah seperti berikut:

a) Memastikan kelancaran operasi KDN dan meminimumkan kerosakan atau kemusnahan;
b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
c) Mencegah salah guna atau kecurian aset ICT Kerajaan;
d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
e) Memperkemaskan pengurusan keselamatan siber KDN.

5 PENYATAAN DASAR

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

Keselamatan siber bermaksud keselamatan ke atas sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan. Keselamatan siber berkait rapat dengan perlindungan ke atas aset ICT sama ada perkakasan, perisian, maklumat, manusia dan perkhidmatan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a) Melindungi maklumat terperingkat 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 daripada sumber yang sah.

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

a) **Kerahsiaan** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan di akses tanpa kebenaran;
b) **Integriti** - Data dan maklumat tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c) **Tidak Boleh Disangkal** - Punca data dan maklumat dari punca yang sah dan tidak boleh disangkal;
d) **Kesahihan** - Data dan maklumat dijamin kesahihannya; dan
e) **Ketersediaan** - Data dan maklumat boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah menjamin keselamatan siber 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.

6 SKOP

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

a) Data dan maklumat boleh di akses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b) Semua data dan maklumat dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, PKS KDN ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KDN. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan didalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KDN;

c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh-contoh adalah seperti berikut:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses;
iii. Perkhidmatan pihak ketiga seperti pembekal *Cloud Service Provider* (CSP) atau *Software-As-A-Service* (SaaS); dan
iv. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif KDN. Contohnya, dokumentasi, prosedur operasi, rekod-rekod KDN, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

e) Manusia

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

f) Premis Komputer dan Komunikasi

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

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

7 PRINSIP-PRINSIP

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

a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan;

b) Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujudkan, menyimpan, mengemas kini, mengubah atau menghapuskan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT;

d) Pengasingan

Tugas mewujudkan, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan mengikut peranan masing-masing bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan peranan antara kumpulan operasi dan rangkaian;

e) Pengauditan

Pengauditan adalah tindakan pemeriksaan dan pengesahan untuk memastikan pengendalian berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan dikendalikan adalah tepat dan sahih. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan*, router, firewall* dan rangkaian ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) Pematuhan

PKS KDN dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber;

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

h) Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

8 PENILAIAN RISIKO KESELAMATAN SIBER

KDN mengambil kira kewujudan risiko ke atas aset ICT akibat daripada ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KDN 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.

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

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

KDN bertanggungjawab melaksanakan dan menguruskan risiko keselamatan siber selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. KDN perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
c) Mengelak risiko dari terjadi dengan mengambil tindakan pencegahan yang sewajarnya; Dan
d) Memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

9 PERKARA 1: POLISI KESELAMATAN MAKLUMAT

9.1 0101 Polisi Keselamatan Maklumat Siber

Objektif	
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan siber selaras dengan keperluan KDN dan perundangan yang berkaitan.	
010101 Pelaksanaan Polisi	**Tanggungjawab**
Pelaksanaan polisi ini akan dijalankan oleh Ketua Setiausaha KDN dan dibantu oleh Jawatankuasa Pemandu ICT	Ketua Setiausaha dan JPICT
010102 Penyebaran Polisi	**Tanggungjawab**
Polisi serta apa-apa pindaan polisi perlu disebar kepada semua warga KDN (termasuk pembekal, pakar runding dan lain-lain).	ICTSO
010103 Penyelenggaraan Polisi	**Tanggungjawab**
Piawaian berhubung dengan penyelenggaraan PKS KDN adalah seperti berikut: a) Polisi ini dikaji semula secara berkala dan apabila berlaku perubahan kepada peraturan yang sedang berkuat kuasa; dan b) Sebarang pindaan dikemuka secara bertulis kepada ICTSO bagi mendapatkan kelulusan pindaan daripada Jawatankuasa Pemandu ICT (JPICT) KDN.	ICTSO
010104 Pengecualian Polisi	**Tanggungjawab**
PKS KDN adalah terpakai kepada warga KDN dan tiada pengecualian diberikan.	Warga KDN dan Pihak Ketiga

10 PERKARA 2: ORGANISASI KESELAMATAN MAKLUMAT

10.1 0201 Infrastruktur Keselamatan Organisasi

Objektif	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS KDN.	
020101 Struktur Organisasi	**Tanggungjawab**
Jawatankuasa Pemandu ICT KDN dan KDN CSIRT adalah bertanggungjawab terhadap pengurusan keselamatan siber KDN. Perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan komitmen pengurusan atasan ke atas keselamatan siber dilaksanakan dengan aktif dan telus; b) Memastikan aktiviti pengurusan keselamatan siber diselaraskan oleh Ketua Setiausaha/Setiausaha Bahagian dari semua peringkat organisasi berdasarkan peranan masing-masing; c) Menetapkan tanggungjawab yang jelas bagi semua warga KDN dalam pengurusan keselamatan siber; d) Memastikan keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksana dan dikaji secara berkala; e) Memastikan jalinan perhubungan/komunikasi dengan pihak yang relevan dipelihara; dan f) Memastikan kajian semula ke atas keselamatan siber dijalankan mengikut peraturan yang ditetapkan.	JPICT KDN, dan KDN CSIRT

020102 Ketua Setiausaha	**Tanggungjawab**
Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut: a) Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber KDN dan semua jabatan/agensi di bawahnya; b) Memperuntukkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah tuju dan strategi keselamatan Siber KDN dan semua jabatan/ agensi di bawahnya; c) Memantau pematuhan PKS KDN; dan d) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KDN.	Ketua Setiausaha
020103 Ketua Pegawai Digital (CDO)	**Tanggungjawab**
Peranan dan tanggungjawab CDO adalah seperti berikut: a) Mengetuai tugas-tugas yang melibatkan pematuhan kepada PKS; b) Memelihara integriti data elektronik c) Menggalakkan perkongsian maklumat dan menyediakan kaedah bagi penyebaran maklumat secara elektronik yang selamat kepada pengguna-penguna yang sah d) Menentukan keperluan keselamatan siber; dan e) Menggalakkan pembudayaan keselamatan siber.	CDO
020104 Pengurus ICT	**Tanggungjawab**
Pengurus ICT KDN ialah pegawai yang dilantik oleh Ketua Setiausaha. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan;	Pengurus ICT

b) Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan secara berkala dan apabila berlaku perubahan kepada peraturan yang sedang berkuat kuasa; dan c) Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.	
020105 Pegawai Keselamatan ICT (ICTSO)	**Tanggungjawab**
Peranan dan tanggungjawab ICTSO adalah seperti berikut: a) Menguatkuasakan dan memantau pelaksanaan PKS KDN; b) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS KDN; c) Mengurus keseluruhan program keselamatan siber KDN; d) Menjalankan tugas pengurusan risiko; e) Menjalankan audit, kajian semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f) Memastikan kajian semula dan pelaksanaan kawalan keselamatan siber selaras dengan keperluan organisasi ; g) Memberi penerangan dan pendedahan berkenaan PKS KDN kepada semua pengguna; h) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i) Melaporkan insiden keselamatan siber kepada Agensi Keselamatan Siber Negara (NACSA) dan memaklumkan kepada CDO; j) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan	ICTSO

siber dan memperakukan langkah-langkah baik pulih dengan segera; k) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan siber; dan l) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020106 Ketua Seksyen BPTM	**Tanggungjawab**
Peranan dan tanggungjawab adalah termasuk seperti berikut: a) Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber KDN kepada ICTSO untuk tindakan; b) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber KDN; dan c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir ICT (*sysadmin*) yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas.	Ketua Seksyen BPTM
020107 Pentadbir ICT	**Tanggungjawab**
Pentadbir ICT KDN adalah berperanan dan bertanggungjawab seperti berikut: a) Memastikan kerahsiaan akaun pentadbir; b) Menjaga kerahsiaan konfigurasi aset ICT; c) Mengambil tindakan yang bersesuaian di dalam tempoh yang ditetapkan apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; d) Mengambil tindakan yang bersesuaian di dalam tempoh yang ditetapkan apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;	Pentadbir ICT

e) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam PKS KDN; f) Memantau aktiviti capaian harian pengguna; g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran, membatalkan atau memberhentikannya dengan serta merta, dan memaklumkan kepada ICTSO dan Setiausaha Bahagian Pengurusan ICT untuk tindakan selanjutnya; h) Menyimpan dan menganalisis rekod jejak audit; dan i) Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam PKS KDN.	
020108 KDN CSIRT	**Tanggungjawab**
Peranan dan tanggungjawab adalah termasuk seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b) Merekod dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai input atau untuk tindakan seterusnya; e) Merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan f) Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada JKICT.	ICTSO dan ahli KDN CSIRT

020109 Warga KDN	**Tanggungjawab**
Warga KDN mempunyai peranan dan tanggungjawab seperti berikut: a) Menjaga kerahsiaan maklumat KDN yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; b) Melaksanakan dan mematuhi prinsip-prinsip PKS KDN; c) Mengetahui dan memahami implikasi keselamatan siber akibat daripada tindakannya; d) Menjaga kerahsiaan kata laluan (*password*); e) Menjalani tapisan keselamatan; f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada KDN CSIRT dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan siber; dan h) Mempersetujui Akuan Pematuhan PKS KDN sebagaimana melalui Laman Rasmi Kementerian Dalam Negeri.	Warga KDN

10.2 0202 Pihak Ketiga

Objektif	
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	**Tanggungjawab**
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Mengenal pasti risiko keselamatan siber dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;	CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pihak Ketiga

b) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; c) Akses kepada aset ICT KDN perlu berlandaskan kepada perjanjian kontrak; dan d) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut dimasukkan di dalam perjanjian yang dimeterai: i. Akuan PKS Warga KDN dan Piha Ketiga / Kontraktor ; ii. Tapisan Keselamatan (*eVetting*); iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek (terpakai bagi keperluan kontrak).	

10.3 0203 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif	
Memastikan keselamatan siber apabila menggunakan peralatan mudah alih dan kerja jarak jauh.	
020301 Pengguna Peralatan Mudah Alih	**Tanggungjawab**
Perkara-perkara berikut dipatuhi: a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; b) Peralatan mudah alih disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan c) Tindakan perlindungan diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Warga KDN

020302 Kerja Jarak Jauh	**Tanggungjawab**
Perkara-perkara berikut dipatuhi: a) Capaian rangkaian Kerja Jarak Jauh untuk tujuan rasmi perlu didaftarkan dan perlu mematuhi peraturan semasa; dan b) Pengguna tertakluk kepada polisi yang ditetapkan di dalam PKS KDN;	Warga KDN
020303 Bawa Peranti Sendiri (BYOD)	**Tanggungjawab**
Perkara-perkara berikut dipatuhi: a) Memastikan peranti peribadi yang dibenarkan untuk digunakan seperti komputer riba, telefon pintar, dan tablet untuk tujuan rasmi perlu didaftarkan dan perlu mematuhi peraturan semasa; b) Memastikan pengguna tertakluk kepada syarat dan polisi yang ditetapkan di dalam PKS KDN; dan c) Memastikan pengguna perlu mendapatkan kata laluan bagi menggunakan rangkaian KDN daripada *Helpdesk* IT. Capaian tanpa menggunakan kata laluan yang sah adalah melanggar PKS KDN.	Warga KDN dan Pihak Ketiga

11 PERKARA 3: KESELAMATAN SUMBER MANUSIA

11.1 0301 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif	
Memastikan semua sumber manusia yang terlibat termasuk warga KDN dan Pihak Ketiga memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga KDN dan Pihak Ketiga mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
030101 Sebelum Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga KDN serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk warga KDN dan pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	ICTSO, Bahagian Pengurusan Sumber Manusia, Warga KDN, dan Pihak Ketiga
030102 Dalam Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan warga KDN serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KDN; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada warga KDN secara berterusan dalam melaksanakan tugas-	ICTSO, Bahagian Pengurusan Sumber Manusia, Warga KDN, dan Pihak Ketiga

tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau pekeliling yang berkaitan; d) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga KDN dan pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KDN; e) Memastikan warga KDN dan pihak ketiga bertanggungjawab dalam pemeliharaan dan perlindungan Maklumat Peribadi mengikut perundangan, peraturan dan kontrak yang ditetapkan oleh Pihak KDN; dan f) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan siber.	
030103 Bertukar Atau Tamat Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan semua aset ICT dikembalikan kepada KDN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KDN.	Bahagian Pengurusan Sumber Manusia, Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT, dan Pengguna

12 PERKARA 4: PENGURUSAN ASET

12.1 0401 Akauntabiliti Aset

Objektif	
Memberi dan menyokong perlindungan yang bersesuaian ke atas penggunaan aset ICT KDN.	
040101 Inventori Aset	**Tanggungjawab**
Ini bertujuan memastikan pengguna aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dan sentiasa dikemaskini; b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c) Mengenal pasti lokasi semua aset ICT KDN; d) Memastikan peraturan bagi pengendalian aset ICT dikenal pasti, didokumen dan dilaksanakan; dan e) Memastikan penggunaan aset maklumat dengan cara yang selamat dan tidak membahayakan ketersediaan, kebolehpercayaan atau integriti data, perkhidmatan atau sumber. Ini juga bermakna menggunakannya dengan cara yang tidak melanggar undang-undang atau dasar organisasi.	Pengurus ICT dan Warga KDN

12.2 0402 Pengelasan dan Pengendalian Maklumat

Objektif	
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	**Tanggungjawab**
Memastikan maklumat dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai	Warga KDN

peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a) Rahsia besar; b) Rahsia; c) Sulit; d) Terhad; atau e) Terbuka	
040202 Pengendalian Maklumat	**Tanggungjawab**
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah mengambil kira langkah-langkah keselamatan berikut bagi mengawal maklumat yang kritikal daripada diubahsuai atau dipinda tanpa kebenaran: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.	Warga KDN

13 PERKARA 5: KAWALAN CAPAIAN

13.1 0501 Dasar Kawalan Capaian

Objektif	
Mengawal capaian ke atas maklumat.	
050101 Keperluan Kawalan Capaian	**Tanggungjawab**
Memastikan capaian kepada proses dan maklumat dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b) Memastikan kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Memastikan kawalan ke atas maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; d) Memastikan kawalan ke atas kemudahan pemprosesan maklumat;dan e) Mengawal capaian ke atas maklumat berdasarkan keistimewaan akses khas mengikut fungsi tugas dan hak perlu mengetahui sama ada menggunakan teknologi terkini atau secara manual.	CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pentadbir ICT

13.2 0502 Pengurusan Capaian Pengguna

Objektif	
Mengawal capaian pengguna ke atas aset ICT KDN.	
050201 Akaun Pengguna	**Tanggungjawab**
Memastikan Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut dipatuhi: a) Memastikan Akaun yang diperuntukkan oleh KDN sahaja boleh digunakan; b) Memastikan Akaun pengguna mestilah unik dan mencerminkan identiti pengguna; c) Memastikan Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KDN. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; d) Memastikan Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan e) Memastikan Pentadbir ICT boleh membeku dan menamatkan akaun pengguna atas sebab- sebab berikut: i. Bertukar bidang tugas kerja; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	ICTSO, Pemilik Projek, Pentadbir ICT
050202 Hak Capaian	**Tanggungjawab**
Memastikan penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	ICTSO, Pemilik Projek, dan Pentadbir ICT

050203 Pengurusan Kata Laluan	**Tanggungjawab**
Memastikan pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KDN. Sistem pengurusan kata laluan interaktif dan mengambil kira kualiti kata laluan yang dicipta. Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan seperti yang berikut: (a) M-emastikan dalam apa jua keadaan dan sebab, kata laluan dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Memastikan kata laluan perlu sekurang-kurangnya PANJANG Lapan (8) aksara tidak termasuk *non-blank character*, kecuali jika terdapat Autentikasi Pelbagai Faktor (MFA) yang digunakan untuk sistem tersebut; (c) Kata laluan tidak boleh mengandungi nama pengguna atau sebahagian daripada nama pengguna KDN BPTM seperti nama pertama mereka; (d) Semua kata laluan, termasuk kata laluan asal, perlu terdiri sekurang-kurangnya satu (1) aksara daripada sekurang-kurangnya tiga (3) daripada empat (4) kategori berikut: i. Aksara besar (Contohnya, A-Z). ii. Aksara kecil (Contohnya, a-z). iii. Aksara khas bukan alfanumerik (Contohnya, @, #, $, %, ^, &, dan sebagainya). iv. Digit/Nombor dalam *Digit* 10 (Contohnya, 0-9). (e) Kata laluan dan PIN perlu dienkripsi semasa disimpan di pangkalan data;	ICTSO, Pemilik Projek, Pentadbir ICT, dan Pengguna

(f) Memastikan pengguna menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (g) Memastikan penggunaan kata laluan paparan kekunci (*lock screen*) terutamanya pada komputer yang terletak di ruang guna sama; (h) Memastikan kata laluan tidak dipaparkan (*data mask*) semasa dimasukkan, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;	
050204 *Clear Desk* dan *Clear Screen*	**Tanggungjawab**
Memastikan semua maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan maklumat terperingkat sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kemudahan *password screen saver* sekurang-kurangnya 10 minit atau log keluar apabila meninggalkan komputer terutamanya pada komputer yang terletak di ruang guna sama; b) Memastikan dokumen terperingkat disimpan dalam laci atau kabinet fail yang berkunci; dan c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Pengguna

13.3 0503 Kawalan Capaian Rangkaian

Objektif	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
050301 Capaian Rangkaian	**Tanggungjawab**
Memastikan kawalan capaian perkhidmatan rangkaian dijamin selamat dengan: a) Menempatkan atau memasang antara muka yang bersesuaian diantara rangkaian KDN, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	ICTSO dan Pentadbir ICT
050302 Capaian Internet	**Tanggungjawab**
Memastikan perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti pengguna yang perlu dikawal menerusi kawalan pengguna untuk pengesahan pengguna; b) Memastikan penggunaan Internet di KDN dipantau secara berterusan oleh Pentadbir ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KDN; c) Memastikan penggunaan Internet hanyalah untuk kegunaan rasmi sahaja;	ICTSO dan Pentadbir ICT

d) Memastikan laman yang dilayari hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pentadbir ICT yang diberi kuasa; e) Memastikan bahan yang diperoleh dari Internet ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet dinyatakan; f) Memastikan pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; g) Memantau sebarang bahan yang dimuat turun dari Internet digunakan untuk tujuan yang dibenarkan oleh KDN; dan h) Memastikan pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, perjudian atau keganasan.	

13.4 0504 Kawalan Capaian Sistem Pengoperasian

Objektif	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
050401 Capaian Sistem Pengoperasian	**Tanggungjawab**
Memastikan kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b) Merekodkan capaian yang berjaya dan gagal. Memastikan kaedah-kaedah yang digunakan mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Menghadkan dan mengawal penggunaan program; dan d) Menghadkan tempoh capaian (*session timed-out*) ke sesebuah aplikasi berisiko tinggi.	ICTSO dan Pentadbir ICT

13.5 0505 Kawalan Capaian Aplikasi dan Maklumat

Objektif	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.	
050501 Capaian Aplikasi dan Maklumat	**Tanggungjawab**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut dipatuhi: a) Memastikan pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b) Memantau setiap aktiviti capaian sistem maklumat dan aplikasi pengguna direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c) Memantau setiap aktiviti capaian kepada sistem dan aplikasi yang berisiko tinggi dihadkan kepada pengguna yang sah sahaja. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; dan d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	ICTSO, Pemilik Projek, dan Pentadbir ICT

13.6 0506 Kawalan Capaian Sistem Pangkalan Data

Objektif	
Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di pangkalan Data.	
050601 Capaian Pangkalan Data	**Tanggungjawab**
Bertujuan untuk memastikan capaian ke atas pangkalan data dan data dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan mampu menyokong pengesahan pengguna, mewujudkan jejak audit ke atas semua capaian, menjana amaran (*alert*), pengesahan capaian dan penyimpanan data. Perkara-perkara berikut dipatuhi: a) Memastikan capaian ke atas pangkalan data dikawal; b) Memastikan penggunaan perisian yang membolehkan capaian terus ke pangkalan data secara pihak ketiga sama ada melalui perisian web atau sebagainya adalah tidak dibenarkan; c) Mewujudkan pengenalan diri (ID) yang unik bagi setiap pengguna dan hanya digunakan untuk pengguna berkenaan sahaja; dan d) Memastikan aplikasi yang perlu mengakses ke pangkalan data dilaksanakan secara berkala dan perlu menggunakan pengenalan diri yang berbeza daripada pengenalan diri pembangun aplikasi dan pentadbir pangkalan data.	ICTSO, Pemilik Projek dan Pentadbir ICT

14 PERKARA 6: KAWALAN KRIPTOGRAFI

14.1 0601 Kawalan Kriptografi

Objektif	
Melindungi kerahsiaan, integriti dan kesahihan maklumat kawalan kriptografi.	
060101 Enkripsi	**Tanggungjawab**
Memastikan dokumen terperingkat perlu dienkripsikan oleh Pengguna bagi pengunaan secara elektronik	ICTSO, Pengguna
060102 Pengurusan Infrastruktur Kunci Awam (PKI)	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan penggunaan sijil digital digunakan bagi capaian sistem mengikut kesesuaian dan keperluan keselamatan siber; b) Memastikan sijil digital disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c) Memastikan perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d) Memastikan sebarang perubahan kepada pemilik atau kehilangan/kerosakan dilaporkan kepada pemilik **Infrastruktur Kunci Awam (PKI**) berkenaan. e) Memastikan penggunaan enkripsi bagi *media storage* pangkalan data.	Pengguna dan Pihak Ketiga

15 PERKARA 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN

15.1 0701 Keselamatan Kawasan

Objektif	
Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
070101 Kawalan Kawasan	**Tanggungjawab**
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan kawasan keselamatan fizikal dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan *perimeter* (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera; d) Mengehad jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan;	CDO, Pengurus ICT, ICTSO, dan Bahagian Khidmat Pengurusan

j) Merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau- bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	
070102 Kawalan Masuk Fizikal	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan warga KDN memakai atau mengenakan kad pas keselamatan sepanjang waktu bertugas; b) Memastikan semua kad pas keselamatan diserahkan semula kepada Unit Pentadbiran apabila pengguna berhenti atau bersara; c) Memastikan setiap pelawat perlu mendaftar dan mendapatkan pas pelawat di pintu masuk ke kawasan atau tempat berurusan dan dikembalikan semula selepas tamat lawatan; d) Memastikan kehilangan pas pelawat dilaporkan dengan segera kepada Pengawal Keselamatan; dan e) Memastikan hanya kakitangan dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT tertentu KDN.	CDO, ICTSO, Bahagian Khidmat Pengurusan Warga KDN dan Pelawat

070103 Kawasan Terperingkat	**Tanggungjawab**
Memastikan kawasan terperingkat ditakrifkan sebagai kawasan yang menempatkan aset ICT berisiko tinggi dan meliputi kawasan premis atau sebahagian daripada premis di mana maklumat terperingkat KDN disimpan, diuruskan atau di mana kerja melibatkan maklumat terperingkat dijalankan. Akses ke kawasan terperingkat adalah dihadkan dengan kebenaran. Memastikan pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	CDO, Pengurus ICT, ICTSO, Bahagian Khidmat Pengurusan, Warga KDN dan Pihak Ketiga

15.2 0702 Keselamatan Peralatan

Objektif	
Melindungi peralatan ICT KDN daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
070201 Peralatan ICT	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan warga KDN menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Memastikan warga KDN bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Memastikan warga KDN dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Memastikan warga KDN dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir ICT; e) Memastikan warga KDN adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f) Warga KDN mesti memastikan perisian antivirus di komputer yang dipertanggungjawabkan kepada pengguna sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan luaran yang digunakan; g) Mewajibkan penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Memastikan peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);	ICTSO, Pentadbir ICT, dan Warga KDN

i) Memastikan semua peralatan ICT disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; j) Memastikan semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; k) Memastikan peralatan ICT yang hendak dibawa keluar dari premis KDN, (kecuali penggunaan komputer riba atas urusan bekerja) perlulah mendapat kebenaran dari Pentadbir ICT dan direkodkan seperti yang dinyatakan dalam Satu Pekeliling Perbendaharaan (1PP) bagi tujuan pemantauan; l) Memastikan peralatan ICT yang hilang dilaporkan kepada ICTSO dan Pengurus ICT dengan segera mengikut Satu Pekeliling Perbendaharaan (1PP) sedia ada; m) Memastikan sebarang kerosakan peralatan ICT dilaporkan kepada Pentadbir ICT untuk dibaik pulih; n) Melarang konfigurasi alamat IP diubah daripada alamat IP yang telah ditetapkan; o) Memastikan warga KDN bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan digunakan sepenuhnya bagi urusan rasmi sahaja; p) Warga KDN memastikan semua perkakasan komputer, pencetak, projektor dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; q) Memastikan sebarang bentuk penyelewengan atau salah guna peralatan ICT dilaporkan kepada ICTSO; dan r) Memastikan semua pergerakan aset ICT KDN direkodkan.	

070202 Media Storan	**Tanggungjawab**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti CDROM, *thumb drive* dan media storan lain. Langkah-langkah pencegahan seperti berikut diambil untuk memastikan kerahsiaan, integriti dan ketersediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat: a) Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Memastikan akses untuk memasuki kawasan penyimpanan media adalah terhad kepada pegawai yang dibenarkan sahaja; c) Memastikan semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Memastikan semua media storan yang mengandungi maklumat terperingkat disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan; e) Memastikan pergerakan media storan direkodkan; f) Memastikan perkakasan *backup* diletakkan di tempat yang terkawal; g) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Memastikan penghapusan maklumat atau kandungan media mestilah mendapat kelulusan Jawatankuasa Pelupusan; i) Memastikan semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat.	ICTSO, Pentadbir ICT, dan Warga KDN

070203 Media Perisian dan Aplikasi	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar, sumber terbuka (*OSS*) dan di bawah Hak Cipta Terpelihara. Pengguna adalah dilarang memuat naik, memuat turun, menyimpan dan menggunakan perisian yang tidak sah (*pirated software*); dan b) Memastikan lesen perisian (registration code, serials, CD-keys) perlu disimpan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan Kod sumber (source code) sesuatu sistem disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT, dan Warga KDN
070204 Penyelenggaraan Peralatan ICT	**Tanggungjawab**
Perkakasan diselenggara dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua perkakasan yang di selenggara mematuhi spesifikasi pengeluar yang telah ditetapkan; b) 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) Memastikan semua perkakasan disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e) Memastikan semua penyelenggaraan mestilah mendapat kebenaran daripada Pentadbir ICT berkenaan; f) Memastikan semua aktiviti penyelenggaraan perlu direkodkan; dan	CDO, ICTSO, Pengurus ICT, Pemilik Projek, Pentadbir ICT

g) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
070205 Peminjaman Perkakasan ICT Untuk Kegunaan Di Luar Pejabat	**Tanggungjawab**
Perkakasan ICT yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a) Memastikan peralatan ICT yang dibawa keluar pejabat mestilah mendapat kelulusan Bahagian Pengurusan Teknologi Maklumat dan tertakluk kepada tujuan yang dibenarkan; dan b) Memastikan aktiviti peminjaman dan pemulangan peralatan ICT mestilah direkodkan.	Pengurus ICT dan Warga KDN
070206 Peralatan Di Luar Premis	**Tanggungjawab**
Bagi perkakasan yang dibawa keluar dari premis KDN, langkah-langkah keselamatan diadakan dengan mengambil kira risiko yang wujud di luar kawalan KDN: a) Memastikan peralatan perlu dilindungi dan dikawal sepanjang masa; b) Memastikan penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan; dan c) Memastikan kehilangan peralatan ICT perlu dilaporkan mengikut peraturan semasa yang ditetapkan.	Warga KDN

070207 Pelupusan Perkakasan	**Tanggungjawab**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KDN. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KDN: a) Memastikan semua kandungan peralatan khususnya yang mengandungi maklumat terperingkat dihapuskan terlebih dahulu sebelum dilupuskan sama ada melalui kaedah: i. Penyingkiran (*purging*) seperti *secure erase* atau *degaussing*; atau ii. Pemusnahan media secara fizikal (*destroying*) seperti penghancuran (*disintegration*), kisaran halus (*pulverization)*, peleburan dan pembakaran. b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Memastikan peralatan ICT yang akan dilupuskan dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d) Jawatankuasa pelupusan Aset mengenal pasti sama ada peralatan tertentu boleh dilupus atau sebaliknya; e) Memastikan pengurus ICT bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; f) Memastikan peralatan yang hendak dilupus disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;	Pengurus ICT dan Warga KDN

g) Pelupusan peralatan ICT dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; h) Warga KDN bertanggungjawab memastikan segala maklumat terperingkat di dalam komputer disalin pada media storan kedua seperti *external hard disk* atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan; dan i) Memastikan warga KDN adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; ii. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya; iii. Memindah keluar dari KDN mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KDN.	

15.3 0703 Keselamatan Persekitaran

Objektif	
Melindungi aset ICT KDN daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
070301 Kawalan Persekitaran	**Tanggungjawab**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubah suai, pembelian mematuhi garis panduan, tatacara dan prosedur yang sedang berkuat kuasa. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Memastikan semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pengesan kebakaran, alat pencegah kebakaran dan pintu kecemasan; c) Memastikan peralatan perlindungan dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Memastikan semua bahan mudah terbakar, cecair bahan atau peralatan lain yang boleh merosakkan peralatan ICT, diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT; dan e) Memastikan semua peralatan perlindungan disemak dan diuji sekurang-kurangnya sekali dalam setahun atau mengikut keperluan. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	CDO, ICTSO dan Bahagian Khidmat Pengurusan

070302 Bekalan Kuasa	**Tanggungjawab**
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua peralatan ICT dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai; b) Memastikan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Memastikan semua peralatan sokongan bekalan kuasa diperiksa, diuji dan diselenggara secara berjadual.	CDO, ICTSO, Pengurus ICT dan Bahagian Khidmat Pengurusan
070303 Keselamatan Kabel	**Tanggungjawab**
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	ICTSO, dan Pentadbir ICT

070304 Prosedur Kecemasan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan warga KDN membaca, memahami dan mematuhi prosedur kecemasan yang sedang berkuatkuasa; dan b) Kecemasan persekitaran seperti kebakaran dilaporkan kepada Pegawai Keselamatan.	ICTSO, Pegawai Keselamatan dan Warga KDN

15.4 0704 Keselamatan Dokumen

Objektif
Melindungi maklumat KDN daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.

070401 Kawalan Persekitaran	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti setiap dokumen difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; b) Memastikan pergerakan fail dan dokumen direkodkan dan perlulah mengikut prosedur keselamatan; c) Mengenal pasti kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d) Memastikan pelupusan dokumen mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan e) Memastikan dokumen / rekod elektronik terperingkat perlu dienkripsikan bagi penghantaran secara elektronik.	Warga KDN dan Pihak Ketiga

16 PERKARA 8: KESELAMATAN OPERASI

16.1 0801 Pengurusan Prosedur Operasi

Objektif	
Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
080101 Pengendalian Prosedur	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan masih diguna pakai didokumenkan, disimpan dan dikawal; b) Memastikan setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c) Memastikan semua prosedur dikemaskini dari semasa ke semasa atau mengikut keperluan; dan d) Memastikan pengguna mematuhi prosedur yang telah ditetapkan.	Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT, Pengguna
080102 Kawalan Perubahan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Ketua Seksyen BPTM terlebih dahulu; b) Memastikan aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT (perkakasan, perisian, sistem aplikasi, pangkalan data dan maklumat) dikendalikan oleh Pentadbir	Pengurus ICT, ICTSO, Ketua Seksyen BPTM, Pemilik Projek, Pentadbir ICT, dan Warga KDN

ICT atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c) Memastikan semua aktiviti pengubahsuaian komponen sistem ICT mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Memastikan semua aktiviti perubahan atau pengubahsuaian direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
080103 Pengasingan Tugas dan Tanggungjawab	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; dan b) Pembangunan, pengujian dan operasi (penggunaan sistem) mesti diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah ke atas sistem yang sedang beroperasi.	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, dan Pentadbir ICT

16.2 0802 Perancangan dan penerimaan Sistem

Objektif	
Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
080201 Pengurusan Kapasiti	**Tanggungjawab**
Bagi meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem, berikut adalah perkara yang mesti diambil kira: a) Kapasiti sesuatu Aset ICT termasuk peranti, sistem pengoperasian, sistem aplikasi mestilah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan	JPICT, Pengurus ICT, ICTSO, Ketua Seksyen BPTM, Pemilik Projek, dan Pentadbir ICT

bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; b) Aset ICT *EOL*, *EOS* atau *BER* yang mendedahkan KDN kepada risiko keselamatan siber atau mengganggu perkhidmatan hendaklah dikenal pasti dan dikawal bagi meminimumkan risiko; dan c) Keperluan kapasiti ini juga perlu mengambil kira ciri- ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. d) Memastukan perlaksanaan redundansi bagi kemudahan pemprosesan maklumat untuk memenuhi keperluan ketersediaan.	
080202 Penerimaan Sistem	**Tanggungjawab**
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubah suai) memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	JPICT, Pemilik Projek, Pengguna

16.3 0803 Perisian Hasad (*Malware*)

Objektif	
Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian jahat seperti *virus, trojan, malware* dan sebagainya.	
080301 Perlindungan dari Perisian Hasad	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang sistem keselamatan untuk mengesan dan mencegah perisian atau program berbahaya mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuat kuasa;	ICTSO, Pemilik Project, Pentadbir ICT, Warga KDN dan Pihak Ketiga

c) Mengimbas semua perisian atau sistem dengan perisian keselamatan seperti antivirus sebelum menggunakannya; d) Mengemaskini *signature* dan versi perisian keselamatan yang terkini; dan e) Memastikan penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	

16.4 0804 Pengurusan Keselamatan Konfigurasi

Objektif	
Untuk memastikan dan mengekalkan integriti sistem IT melalui kawalan proses permulaan, perubahan dan pemantauan konfigurasi sistem dalam keadaan selamat dan terkini.	
080401 Keselamatan Konfigurasi	**Tanggungjawab**
Bagi memastikan sistem dapat dikonfigurasikan dengan selamat, perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pelan aktiviti konfigurasi sistem IT dijalankan berdasarkan garis dasar dan keperluan organisasi; b) Mengenalpasti dan melaksanakan konfigurasi merangkumi pembangunan, semakan, pengujian dan kelulusan mengikut garis dasar yang selamat untuk konfigurasi sistem IT; c) Memastikan perubahan konfigurasi sistem dikenalpasti, disemak dan diluluskan sebelum pelaksanaan. Fasa ini juga merangkumi keupayaan pelan sandaran sekiranya perlu; d) Menyemak dan memantau samada konfigurasi sedia adalah mematuhi dengan garis dasar yang diluluskan;dan e) Menyimpan salinan sandaran konfigurasi di lokasi yang berlainan dan selamat.	ICTSO, Pemilik Projek, dan Pentadbir ICT

16.5 0805 *Data Leakage Prevention (DLP)*

Objektif	
Mencegah daripada kebocoran data secara tidak sah dan melindungi pengguna daripada menghantar maklumat sensitif atau maklumat penting keluar daripada rangkaian KDN bagi mengekalkan integriti maklumat dan perkhidmatan komunikasi.	
080501 Pencegahan Kebocoran Data	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melindungi data KDN melalui pengurusan penggunaan, penghantaran dan penyimpanan; b) Memastikan garis panduan untuk pengendalian insiden DLP dilaksanakan; c) Memastikan penyelia insiden memahami tanggungjawab berkaitan pengendalian DLP;dan d) Senarai informasi berkaitan polisi DLP termasuk seperti berikut tetapi tidak terhad kepada: i) Dokumen elektronik (.pdf, word, Excel, PPT dan dll) ii) Informasi pengkalan data dan sistem iii) Media simpanan iv) E-mel	ICTSO, Pemilik Projek, Pentadbir ICT dan Penyelia Insiden.

16.6 0806 SANDARAN (*BACKUP*)

Objektif	
Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa dan memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
080601 Sandaran Maklumat	**Tanggungjawab**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan sandaran dilakukan seperti berikut:	ICTSO, Pemilik Projek, dan Pentadbir ICT

e) Membuat salinan sandaran dan menguji secara berkala berdasarkan prosedur *backup*; f) Membuat salinan sandaran ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan penduaan, sama ada secara harian, mingguan, bulanan dan tahunan bergantung kepada tahap kritikal maklumat g) Menguji sistem sandaran dan prosedur *restore* yang sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan;dan h) Merekod dan menyimpan salinan sandaran di lokasi yang berlainan dan selamat.	

16.7 0807 Pengurusan Media

Objektif	
Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
080701 Pengurusan Media	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat serta bersesuaian dengan kandungan maklumat;	Pentadbir ICT

f) Memastikan media yang mengandungi maklumat terperingkat dihapus atau dimusnahkan mengikut prosedur yang ditetapkan;dan g) Penghantaran atau pemindahan media ke luar pejabat direkodkan dan mendapat kebenaran daripada Ketua Seksyen BPTM terlebih dahulu.	
080702 Keselamatan Dokumen	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan penyimpanan dokumen mempunyai ciri-ciri keselamatan; b) Menyediakan dan memantapkan keselamatan dokumen; dan c) Mengawal dan merekodkan semua aktiviti capaian dokumen sedia ada.	ICTSO, Pemilik Projek, Pentadbir ICT

16.8 0808 Pemantauan

Objektif	
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080801 Pengauditan dan Forensik ICT	**Tanggungjawab**
Bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a) Mengenal pasti sebarang percubaan pencerobohan kepada sistem ICT KDN; b) Mengenal pasti serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss);* c) Mengenal pasti pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana- mana pihak;	ICTSO, Pentadbir ICT, KDN CSIRT

d) Mengenal pasti aktiviti melayari, menyimpan atau mengedar bahan-bahan pornografi, perjudian, berunsur fitnah dan propaganda anti kerajaan; e) Mengenal pasti aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Mengenal pasti aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g) Mengenal pasti aktiviti penyalahgunaan akaun e-mel; dan h) Mengenal pasti aktiviti penukaran alamat IP (IP *Address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir ICT.	
080802 Jejak Audit	**Tanggungjawab**
Setiap sistem mestilah mempunyai jejak audit (audit *trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit mengandungi maklumat- maklumat berikut: a) Mencatat rekod setiap aktiviti transaksi; b) Mencatat rekod setiap aktiviti perlu disimpan untuk tempoh masa yang dipersetujui JPICT; c) Mengenal pasti maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; d) Mengenal pasti aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; e) Mengenal pasti maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; dan f) Memastikan waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KDN atau domain keselamatan	ICTSO, Pentadbir ICT

perlu diselaraskan dengan satu sumber waktu yang dipersetujui. Pentadbir ICT menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
080803 Sistem Log	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c) Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan.	Pentadbir ICT
080804 Pemantauan Log	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Memastikan kemudahan merekod dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; c) Memastikan aktiviti pentadbiran dan operator sistem perlu direkodkan; d) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;dan	ICTSO, Pentadbir ICT

e) Memastikan waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KDN atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

17 PERKARA 9: KESELAMATAN KOMUNIKASI

17.1 0901 Pengurusan Keselamatan Rangkaian

Objektif	
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
090101 Kawalan Rangkaian	**Tanggungjawab**
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan peralatan rangkaian diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; b) Mengawal capaian kepada peralatan rangkaian dan menghadkan capaian kepada pengguna yang dibenarkan sahaja; c) Memastikan pengasingan segemen rangkaian bagi pengguna dan sistem maklumat yang dilaksanakan didalam rangkaian KDN; d) Memastikan pelaksanaan konfigurasi pada peralatan rangkaian dan keselamatan perlu dilaksanakan bagi melindungi capaian maklumat; e) Pemasangan yang dapat merekod penggunaan rangkaian seperti perisian *sniffer* atau *network analyser* dan peralatan lain adalah dilarang kecuali mendapat kebenaran Ketua Seksyen BPTM; f) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum;	ICTSO, Pentadbir ICT

g) Memastikan sebarang penyambungan rangkaian daripada pihak ketiga ke dalam sistem rangkaian KDN mendapat kebenaran Ketua Seksyen BPTM; h) Memastikan semua penggunaan rangkaian tanpa wayar (*wireless*) di KDN mematuhi pekeliling yang berkenaan; i) Menapis semua trafik keluar dan masuk rangkaian menggunakan peralatan keselamatan di bawah kawalan KDN; j) Melaksanakan kawalan penapisan web yang sesuai untuk menyekat dan mengawal akses kepada tapak web luaran dan mencegah ancaman keselamatan; k) Aktiviti melayari laman sesawang yang dilarang seperti pornografi, perjudian atau keganasan perlu disekat menggunakan peralatan keselamatan; l) Melaksanakan konfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; m) Memastikan operasi rangkaian diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan; dan n) Pengurusan keselamatan perkhidmatan KDN tidak membenarkan penggunaan perkhidmatan perkomputeran awan dan haruslah merujuk kepada Garis Panduan Penkomputeran Awan *(Cloud Computing)*. Walaubagaimanapun, KDN tidak membenarkan penggunaan perkhidmatan pengkomputeran awan untuk menyimpan data buat masa kini.	

17.2 0902 Pengurusan Pertukaran Maklumat

Objektif	
Memastikan keselamatan pertukaran maklumat dan perisian antara KDN dan pihak ketiga terjamin.	
090201 Polisi, Proses dan Prosedur Pertukaran Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan polisi dan prosedur kawalan pertukaran maklumat untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan b) Melindungi aset ICT KDN yang mengandungi maklumat terperingkat daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KDN.	ICTSO, Pemilik Projek, Pentadbir ICT, dan Warga KDN
090202 Perjanjian Pertukaran Maklumat	
a) Mengenal pasti jenis aset maklumat yang dibenarkan untuk dikongsi oleh KDN serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; b) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (KDN dan pihak ketiga) untuk mendedahkan mereka dengan polisi, proses, dan prosedur berkaitan keselamatan siber; c) Mewujudkan kontrak rasmi bersama pihak ketiga bagi menjamin keselamatan siber KDN di samping segala urusan bersama pembekal dilaksanakan secara rasmi; dan d) Mewujudkan perjanjian yang jelas agar pihak ketiga dan pembekal memastikan keselamatan siber yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya memulangkan kembali semua aset maklumat sekiranya kontrak mereka tamat atau ditamatkan.	ICTSO, Pemilik Projek, Pentadbir ICT, dan Warga KDN

090203 Pengurusan Mel Elektronik	**Tanggungjawab**
Penggunaan mel elektronik (e-mel) di KDN dipantau secara berterusan oleh Pentadbir e-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam oleh Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan". Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan akaun atau alamat e-mel yang diperuntukkan oleh KDN bagi urusan rasmi sahaja; b) Memastikan penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; c) Megelakkan daripada membuka e-mel daripada penghantar yang tidak diketahui atau diragui; d) Mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; e) Mengawal setiap e-mel rasmi yang dihantar atau diterima disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; f) Memastikan tarikh dan masa sistem komputer adalah tepat; dan g) Pengguna bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	Pengguna

17.3 0903 Perkhidmatan Dalam Talian (*Online*)

Objektif	
Mengawal aplikasi dan maklumat dalam perkhidmatan ini supaya sebarang risiko seperti penyalahgunaan maklumat, serta pindaan yang tidak sah dapat dihalang.	
090301 Perkhidmatan Dalam Talian (*Online*)	**Tanggungjawab**
Bagi menggalakkan pertumbuhan perkhidmatan dalam talian serta sebagai menyokong hasrat kerajaan mengoptimumkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan maklumat yang terlibat dalam transaksi dalam talian perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b) Memastikan maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c) Memastikan Kerahsiaan dan Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan dilindungi, misalnya dengan penggunaan Sijil Digital Pelayan yang sah atau PKI, untuk mencegah sebarang pindaan yang tidak diperakukan.	CDO, ICTSO, Pemilik Projek, Pengguna dan Pelanggan
090302 Maklumat Umum	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan siber adalah seperti berikut: a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;	CDO, ICTSO, Pemilik Projek, Pengguna dan Pelanggan

b) Mengesahkan dan mendapat kelulusan untuk segala maklumat yang hendak dipaparkan sebelum dimuat naik ke laman web; dan c) Menguji sistem yang boleh diakses oleh orang awam terlebih dahulu untuk memastikan segala maklumat yang dipaparkan adalah seperti yang telah disah dan diluluskan sebelum dimuat naik ke laman web.	

17.4 0904 Media Sosial

Objektif	
Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.	
090401 Media Sosial	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut: a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; b) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan. Warga KDN boleh merujuk kepada dokumen Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam oleh MAMPU	Warga KDN dan Pihak Ketiga

18 PERKARA 10: PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

18.1 1001 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif	
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan siber yang bersesuaian.	
100101 Keperluan Keselamatan Sistem Maklumat	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Maklumat mengenai Pengurusan Keselamatan Projek adalah mengikut Garis Panduan Pengurusan Projek ICT (PPrISA) a) Memastikan perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Memastikan perlaksanann redundansi bagi kemudahan pemprosesan maklumat untuk memenuhi keprluan ketersediaan; c) Memastikan ujian keselamatan dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta sistem output untuk memastikan data yang telah diproses adalah tepat; d) Memastikan aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan e) Memastikan semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya diuji terlebih dahulu dari	CDO, ICTSO, Ketua Seksyen BPTM, dan Pemilik Projek

segi fungsi dan kawalan keselamatan bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
100102 Validasi Data Input dan Output	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, dan Pengguna

18.2 1002 Keselamatan dalam Proses Pembangunan dan Proses Sokongan

Objektif	
Memastikan supaya sistem maklumat dan aplikasi dikawal dan dikendalikan dengan baik dan selamat	
100201 Kawalan Sistem Maklumat dan Aplikasi	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi dikawal, diuji, direkod dan disahkan sebelum diguna pakai; b) Memastikan proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; c) Mengkaji dan menguji semula aplikasi kritikal apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi; d) Memastikan pentadbir ICT perlu memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga;	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, Pentadbir ICT dan Pembekal

e) Mengawal perubahan dan/atau pindaan ke atas perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; f) Memastikan data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; g) Memastikan akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pembangun sistem yang dibenarkan sahaja; dan h) Menghalang sebarang peluang untuk membocorkan maklumat.	

18.3 1003 Pembangunan Sistem Aplikasi

Objektif	
Memastikan pembangunan sistem aplikasi secara *in-house* dan *outsource* perlu diselia dan dipantau untuk memastikan ia mengikut jadual dan prosedur yang telah ditetapkan.	
100301 Prosedur Pembangunan Sistem Aplikasi	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pembangunan sistem menggunakan teknik *secure coding*; dan b) Memastikan semua sistem baru dan penambahbaikan sistem menjalani ujian penerimaan sistem bagi memastikan garis panduan keselamatan dipenuhi serta lulus *User Acceptance Test (UAT)* dan *Final Acceptance Test (FAT)* sebelum sistem diguna pakai.	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, Pentadbir ICT

100302 Pembangunan Perisian Secara *Outsource*	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan kod sumber, data/maklumat, prosedur dan dokumen yang dibangunkan oleh Pihak Ketiga adalah hak milik KDN; dan b) Setiap sistem, aplikasi dan perisian mematuhi garis panduan keselamatan dan lulus *User Acceptance Test* (UAT) dan *Final Acceptance Test* (FAT).	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, Pentadbir ICT dan Pembekal

18.4 1004 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif	
Memastikan kawalan teknikal keterdedahan (*vulnerability*) adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
100401 Kawalan dari Ancaman Teknikal	**Tanggungjawab**
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan (*vulnerability*) yang terkini ke atas sistem maklumat yang digunakan; b) Menilai tahap teknikal keterdedahan (*vulnerability*) bagi mengenal pasti tahap risiko yang bakal dihadapi; c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan; dan d) Melaksanakan aktiviti *Security Posture Assessment* (SPA) perlu dilaksanakan sekurang-kurangnya sekali setahun.	ICTSO, Ketua Seksyen BPTM, Pemilik Projek, Pentadbir ICT, Pembekal

18.5 1005 Pembangunan Aplikasi Mudah Alih

Objektif	
Menerangkan perkara yang perlu dipatuhi dalam membangunkan aplikasi mudah alih.	
100501 Prosedur Integrasi Pembangunan Aplikasi Mudah Alih	**Tanggungjawab**
Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.	ICTSO, Ketua Seksyen BPTM, Pemilik Projek

19 PERKARA 11: HUBUNGAN PEMBEKAL

19.1 1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal

Objektif	
Memastikan aset ICT yang boleh dicapai oleh pembekal dilindungi.	
110101 Keselamatan Maklumat Berkaitan Hubungan Pembekal	**Tanggungjawab**
Seksyen ini menjelaskan keperluan untuk mendokumentasikan strategi mitigasi risiko keselamatan siber bila mana pembekal dibenarkan untuk akses ke aset KDN. Perkara yang perlu dipatuhi termasuk yang berikut: a) Mengenal pasti jenis aset maklumat yang dibenarkan untuk diakses oleh pembekal serta melakukan pemantauan dan pengawalan terhadap aset tersebut secara berterusan; b) Mengadakan latihan kesedaran kepada semua pihak yang terlibat (KDN dan pembekal) untuk mendedahkan mereka dengan polisi, proses, dan prosedur berkaitan keselamatan siber; c) Mewujudkan mekanisma/proses pengurusan pembekal dengan mengambil kira aspek keselamatan siber sebagai teras; d) Memastikan pemantauan berterusan dilakukan terhadap semua pembekal dengan melaksanakan pengukuran prestasi dan pematuhan terhadap garis panduan keselamatan siber; e) Mewujudkan kontrak rasmi bersama pembekal bagi menjamin keselamatan siber KDN di samping segala urusan bersama pembekal dilaksanakan secara rasmi; dan f) Mewujudkan perjanjian yang jelas agar pihak pembekal memastikan keselamatan siber yang digunakan terjamin sepanjang akses dibenarkan dan seterusnya	Bahagian Perolehan, Penasihat Undang-Undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT dan Pembekal

memulangkan kembali semua aset maklumat sekiranya kontrak mereka tamat atau ditamatkan.	
110102 Rangkaian Pembekal ICT	**Tanggungjawab**
Seksyen ini menjelaskan kandungan perjanjian bersama pembekal yang perlu diwujudkan bagi memastikan risiko keselamatan siber berkaitan rangkaian pembekal khidmat ICT dan produk diambil kira. Perkara yang perlu dipatuhi termasuk yang berikut: a) Mengenal pasti keperluan keselamatan siber khusus berkaitan dengan perolehan rangkaian pembekal perkhidmatan dan produk ICT sebagai tambahan kepada keperluan umum keselamatan siber berkaitan hubungan sub-pembekal; b) Memastikan rangkaian pembekal yang terlibat dalam menyediakan perkhidmatan dan produk ICT berkongsi hal berkaitan keselamatan siber (polisi, prosedur, proses) kepada setiap aras pembekal termasuk sub-pembekal atau sub-sub-pembekal; c) Melaksanakan proses pemantauan rangkaian pembekal perkhidmatan dan produk ICT dengan kaedah yang berkesan bagi menjamin keperluan keselamatan siber sentiasa dipatuhi; d) Mendapatkan jaminan bahawa komponen produk yang kritikal boleh berfungsi mengikut spesifikasi dan dikesan sumbernya dari rangkaian pembekal yang pelbagai; dan e) Menguruskan rangkaian pembekal perkhidmatan dan produk ICT bagi menjamin keselamatan siber dan kesinambungan perkhidmatan kerana perubahan trend dan teknologi.	Bahagian Perolehan, Penasihat Undang-Undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek, dan Pembekal

19.2 1102 Pengurusan Penyampaian Perkhidmatan Pembekal

Objektif	
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan siber dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal.	
110201 Perkhidmatan Penyampaian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan di selenggara oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau dan disemak secara berkala; dan c) Mengambil kira Pengurusan perubahan dasar tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Bahagian Perolehan, Penasihat Undang-Undang, JPICT, CDO, ICTSO, Pemilik Projek, Pengurus ICT dan Pembekal
110202 Pemantauan dan Kajian Perkhidmatan Pembekal	**Tanggungjawab**
KDN sentiasa memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal. Perkara-perkara berikut dipatuhi: a) Memantau tahap prestasi perkhidmatan bagi mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan b) Memastikan laporan perkhidmatan yang dihasilkan oleh pembekal dipantau dan status kemajuan dikemukakan kepada KDN.	Bahagian Perolehan, Penasihat Undang-Undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal

110203 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Semua perubahan perkhidmatan pembekal dilaksanakan secara teratur dan mengikut klausa kontrak yang ditetapkan. Perkara-perkara yang perlu diambil kira adalah seperti berikut: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh KDN bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan-perubahan melibatkan rangkaian, teknologi, produk, perkakasan, lokasi serta pertukaran pembekal dan subkontraktor.	Bahagian Perolehan, Penasihat Undang-Undang, JPICT, CDO, Pengurus ICT, ICTSO, Pemilik Projek dan Pembekal

20 PERKARA 12: PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN SIBER

20.1 1201 Mekanisme Pelaporan Insiden Keselamatan Siber

Objektif	
Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan siber.	
120101 Mekanisme Pelaporan	**Tanggungjawab**
Insiden keselamatan siber bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT sama ada perkakasan, perisian atau ke atas kakitangan atau ancaman kemungkinan berlaku kejadian tersebut. Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat KDN dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan siber ICT kepada ICTSO KDN dan Pasukan KDN CSIRT dengan segera: a) Maklumat didapati hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail dan sistem kerap kali gagal; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	ICTSO, KDN CSIRT, Warga KDN dan Pihak Ketiga

Pelaporan insiden keselamatan siber di KDN berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

20.2 1202 Pengurusan Maklumat Insiden Keselamatan Siber

Objektif	
Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan siber.	
120201 Pengurusan Insiden	**Tanggungjawab**
Maklumat mengenai insiden keselamatan siber yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KDN. Bahan-bahan bukti berkaitan insiden keselamatan siber disimpan dan diselenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, melaksanakan aktiviti penduaan secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;	ICTSO, KDN CSIRT

c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu; dan f) Pengurusan insiden yang tidak melibatkan insiden keselamatan siber adalah berdasarkan prosedur pengendalian insiden yang ditetapkan oleh pihak KDN.	

21 PERKARA 13: KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

21.1 1301 Dasar Kesinambungan Perkhidmatan

Objektif	
Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
130101 Pelan Kesinambungan Perkhidmatan	**Tanggungjawab**
Pihak KDN memastikan aspek keselamatan siber dalam Pelan Kesinambungan Perkhidmatan (PKP) dibangunkan, laksanakan dan dikemaskini (proses, prosedur serta kawalan) untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh Ketua Jabatan dan perkara-perkara berikut perlu diberi perhatian: a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan siber; c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan dalam jangka masa yang telah ditetapkan; d) Mendokumentasikan proses dan prosedur yang telah di-persetujui; dan e) Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	CDO, Pengurus ICT, ICTSO, Pasukan Pemulihan Bencana KDN dan Pihak Ketiga

PKP perlu dibangunkan dan mengandungi perkara-perkara berikut: a) Memastikan senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b) Memastikan Senarai kakitangan KDN dan pihak ketiga berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; c) Merekod Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; d) Memastikan Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan e) Menyediakan Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. PKP akan diuji secara berkala atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian PKP dijadualkan dan diuji untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KDN memastikan salinan PKP sentiasa dikemaskini.	

130102 Mengesah, Mengkaji semula dan Menilai Keselamatan Maklumat dalam Pelan Pengurusan Kesinambungan Perkhidmatan	**Tanggungjawab**
KDN mengesahkan kawalan terhadap keselamatan siber dalam pelan Pengurusan Kesinambungan Perkhidmatan (PKP). Semakan kesinambungan kawalan keselamatan dikaji semula secara berkala dan apabila berlaku perubahan kepada peraturan yang sedang berkuat kuasa untuk memastikan pelan berkenaan sahih dan berkesan semasa berlaku gangguan/bencana.	CDO, Pengurus ICT, ICTSO, Pasukan Pemulihan Bencana KDN dan Pihak Ketiga

22 PERKARA 14: PEMATUHAN

22.1 1401 Pematuhan dan Keperluan Perundangan

Objektif	
Meningkatkan tahap keselamatan siber bagi mengelak dari pelanggaran kepada PKS KDN.	
140101 Pematuhan Dasar	**Tanggungjawab**
Warga KDN membaca, memahami dan mematuhi PKS KDN dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di KDN termasuk maklumat yang disimpan di dalamnya adalah hak milik KDN dan KDN berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Pihak KDN berhak tidak memberikan kemudahan ICT jika pematuhan dasar tidak diperakui secara rasmi oleh pengguna. Sebarang penggunaan aset ICT KDN selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KDN.	CDO, Pengurus ICT, ICTSO, Pemilik Projek, Pentadbir ICT, Warga KDN dan pengguna
140102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tanggungjawab**
ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan siber.	ICTSO

140103 Pematuhan Keperluan Audit	**Tanggungjawab**
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO dan Warga KDN
140104 Keperluan Perundangan	**Tanggungjawab**
Memastikan senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di KDN adalah seperti di **Senarai Rujukan dan Perundangan.**	Warga KDN
140105 Pelanggaran Dasar	**Tanggungjawab**
Mengenal pasti pelanggaran PKS KDN boleh dikenakan tindakan tatatertib. Pegawai awam adalah tertakluk kepada akta dan peraturan yang sedang berkuatkuasa seperti Akta Rahsia Rasmi 1972 [Akta 88] dan Arahan Keselamatan Kerajaan.	Warga KDN
140106 Hak Harta Intelek (*Intellectual Property Rights* – IPR)	**Tanggungjawab**
Prosedur-prosedur yang sesuai akan dilaksanakan untuk memastikan keselarasan dengan perundangan, peraturan dan juga keperluan kontrak yang berkaitan dengan *Intellectual Property Rights* (IPR) dan juga pelesenan perisian. KDN akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat.	Warga KDN

Perkara-perkara berikut perlu dipatuhi: a) Memastikan pematuhan terhadap hak cipta yang berkaitan dengan perisian proprietari, dan reka bentuk untuk kegunaan KDN; b) Memastikan pematuhan terhadap pelesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh untuk kegunaan KDN;dan c) Memastikan pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	

22.2 1402 Kajian Keselamatan Maklumat

Objektif	
Memastikan keselamatan siber dilaksanakan mengikut polisi dan prosedur KDN.	
140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	**Tanggungjawab**
Dalam pelaksanaan keselamatan siber KDN, kesemua prosedur, polisi dan proses keselamatan siber disemak apabila terdapat perubahan ketara berlaku dalam pelaksanaannya. ICTSO memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.	JPICT dan ICTSO
140202 Pematuhan Kajian Teknikal	**Tanggungjawab**
Aset ICT sentiasa dikaji supaya selaras dengan pematuhan polisi dan piawaian keselamatan siber KDN (seperti *Security Posture Assessment* – SPA).	ICTSO, Pengurus ICT, Pemilik Projek dan Pentadbir ICT

23 SENARAI RUJUKAN DAN PERUNDANGAN

1. Akta Aktiviti Kerajaan Elektronik 2007
2. Akta Arkib Negara 2003
3. Akta Hak Cipta (Pindaan) 1997
4. Akta Jenayah Komputer 1997
5. Akta Multimedia dan Telekomunikasi 1998
6. Akta Perdagangan Elektronik 2006
7. Akta Perlindungan Data Peribadi 2010
8. Akta Rahsia Rasmi 1972
9. Akta Suruhanjaya Komunikasi & Multimedia 1998
10. Akta Tandatangan Digital 1997
11. Arahan Keselamatan (Semakan dan Pindaan 2017)
12. Arahan no. 24 MKN Dasar & Mekanisme Pengurusan Krisis Siber Negara
13. Arahan no. 26 Pengurusan Keselamatan Siber Negara dan Strategi Keselamatan Siber Malaysia (MCSS).
14. Arahan Teknologi Maklumat 2007 - Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680)
15. Garis Panduan Pengurusan Projek ICT (PPrISA)
16. Garis Panduan Penkomputeran Awan
17. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999
18. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002
19. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT)
20. Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam
21. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan

22. Pekeliling Kemajuan Pentadbiran Awam Bil. 3 Tahun 2015 (Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)])
23. Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2021 -(Dasar Perkongsian Data Sektor Awam) - MAMPU
24. Pekeliling Perbendaharaan (PP) PK 2.1
25. Pekeliling Perkhidmatan Sumber Manusia VERSI 1.0 (2022)
26. Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA)
27. Penerapan Etika Penggunaan Media Sosial Dalam Sektor Awam – MAMPU
28. Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005
29. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987;
30. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
31. Surat Arahan Ketua Pengarah MAMPU 2010 - (Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam)
32. Surat Arahan Ketua Pengarah MAMPU 2011 (Penggunaan Media Jaringan Sosial Di Sektor Awam)
33. Surat Arahan Ketua Pengarah MAMPU 2015 - Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRam App. 2.0 Di Agensi Sektor Awam
34. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimili di Pejabat-Pejabat Kerajaan
35. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976
36. Surat Pekeliling AM Bilangan 2 Tahun 2021 -Garis Panduan Pengurusan Keselamatan Maklumat Awam Melalui Pengkomputeran Awan dalam

Perkhidmatan Awam) pekeliling kemajuan pentadbiran awam bilangan 1 tahun 2021 - dasar komputeran awam sektor awam) - MAMPU

37. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam
38. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan
39. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (espionage)
40. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019