KEMENTERIAN PERPADUAN NEGARA

POLISI KESELAMATAN SIBER KEMENTERIAN DAN AGENSI

Versi 2.0

HAK CIPTA TERPELIHARA KERAJAAN MALAYSIA

PERUTUSAN KETUA SETIAUSAHA
KEMENTERIAN PERPADUAN NEGARA

Assalamualaikum WBT dan Salam Perpaduan,

Terlebih dahulu, saya merakamkan setinggi-tinggi tahniah dan penghargaan kepada semua pegawai ICT Kementerian Perpaduan Negara dan Agensi atas kejayaan menyediakan Polisi Keselamatan Siber (PKS) ini sebagai rujukan rasmi.

Kerajaan komited memperkukuh penyampaian perkhidmatan awam melalui penggunaan ICT secara menyeluruh dan bersepadu.
Namun, kemajuan teknologi juga meningkatkan risiko keselamatan siber yang perlu ditangani secara serius.

Justeru, semua warga Kementerian dan Agensi diseru untuk memahami serta mengamalkan penggunaan ICT secara menyeluruh, berhemah dan selamat. Penerbitan PKS ini diharap menjadi panduan utama dalam melindungi perkakasan, perisian, sistem dan data maklumat organisasi.

PKS bukan sekadar rujukan, tetapi satu kewajipan. Kegagalan mematuhinya boleh dikenakan tindakan tatatertib mengikut peraturan yang berkuatkuasa.

Akhir kata, saya menyeru agar semua pihak memberi kerjasama penuh dalam pelaksanaan PKS ini. Hanya melalui pematuhan menyeluruh, kita dapat memastikan keselamatan ICT terpelihara dan matlamat organisasi tercapai dengan berkesan.

Sekian, terima kasih.

Ketua Setiausaha
Kementerian Perpaduan Negara

PERUTUSAN KETUA PEGAWAI DIGITAL (CDO)
KEMENTERIAN PERPADUAN NEGARA

Assalamualaikum WBT dan Salam Perpaduan,

Syukur ke hadrat Allah SWT kerana dengan izin-Nya, Polisi Keselamatan Siber (PKS) ini berjaya dibangunkan. **Setinggi-tinggi penghargaan saya ucapkan kepada** semua pegawai ICT Kementerian Perpaduan Negara (KPN) dan agensi-agensi yang telah menyumbang kepakaran dan komitmen dalam penyediaan dokumen ini.

PKS ini dirangka berpandukan Garis Panduan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) oleh NACSA, Arahan dan Pekeliling Kerajaan berkaitan Keselamatan, Polisi Keselamatan Siber Jabatan Digital Negara (JDN) dan Kementerian-kementerian lain selaras dengan usaha Kerajaan memperkukuh keselamatan siber sektor awam.

Dokumen ini menjadi rujukan utama yang menetapkan peraturan dan panduan keselamatan siber yang wajib dipatuhi oleh semua pegawai Kementerian dan Agensi dalam pengurusan serta penggunaan aset ICT rasmi.

Selaras dengan transformasi digital, komitmen terhadap keselamatan siber amat penting bagi melindungi maklumat dan aset ICT Kerajaan daripada ancaman yang boleh menjejaskan operasi.

PKS ini terpakai kepada semua pegawai. Pematuhan sepenuhnya adalah tanggungjawab bersama demi menjamin perkhidmatan Kerajaan kekal selamat, cekap dan berintegriti.

Sekian, terima kasih.

Ketua Pegawai Digital
Kementerian Perpaduan Negara

REKOD PINDAAN

Bahagian ini merekodkan maklumat pindaan yang telah dibuat pada dokumen.

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
04/7/2021	1.0		01/1/2022
17/12/2025	2.0	Mesyuarat Jawatankuasa Pemandu Bilangan 7 Tahun 2025	17/12/2025

AKRONIM/TERMA/TAKSIRAN

Bahagian ini merekodkan akronim/terma/taksiran pada dokumen Polisi Keselamatan Siber ini.

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
Agensi	Merujuk kepada Agensi di bawah Kementerian Perpaduan Negara.
Akses Sistem	Mengakses sistem secara back-end seperti aplikasi Remote Desktop , Putty, PHPMyAdmin, HeidiSQL dan lain-lain.
ANM	Arkib Negara Malaysia
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM untuk sebarang kemungkinan adanya virus.
API *(Application Programming Interface*)	Satu set arahan pengaturcaraan dan standard untuk akses menerusi aplikasi web menggunakan perisian aplikasi web.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus.
Bandwidth	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contoh: *video streaming* dan *teleconference.*
BKP	Bahagian Khidmat Pengurusan
BKPSM	Bahagian Khidmat Pengurusan dan Sumber Manusia
BPM	Bahagian Pengurusan Maklumat
BYOD *(Bring Your Own Device)*	Peralatan mudah alih persendirian seperti telefon pintar, *tablet*, komputer riba dan media storan yang digunakan untuk tujuan rasmi.
CC	*Corrective*

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
CDO *(Chief Digital Officer)*	Ketua Pegawai Digital, iaitu pegawai yang dilantik untuk menjadi peneraju dalam merancang, melaksana dan memantau program Kerajaan berasaskan ICT bagi memudahkan pelanggan berurusan dengan agensi Kerajaan. Beliau juga merupakan agen transformasi menerusi inovasi, kreativiti dan inisiatif pembaharuan yang berterusan.
CGSO *(Chief Government Security Office)*	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah agensi Perdana Menteri, Malaysia.
Clear Desk dan *Clear Screen*	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
Content Filtering	Satu teknik yang menyekat atau membenarkan berdasarkan analisis kepada kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian internet dan email.
CSIRT *(Computer Security Incident Response Team)*	Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu agensi pengurusan pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
DRP *(Disaster Recovery Plan)*	Pelan Pemulihan Bencana, iaitu dokumentasi pendekatan berstruktur yang menerangkan bagaimana sesebuah organisasi dengan cepatnya memulakan semula kerja setelah berlakunya bencana. DRP merupakan bahagian penting dalam Pelan Pengurusan Kesinambungan Perkhidmatan yang melibatkan aspek-aspek tertentu organisasi yang bergantung kepada infrastruktur ICT.
E-mel (Mel Elektronik)	Maklumat atau mesej yang dihantar secara elektronik dari satu terminal komputer ke terminal komputer yang lain.
EA *(Enterprise Architecture)*	Suatu amalan untuk menakrifkan dan menjajarkan strategi Bisnes dan ICT menerusi pemahaman, perundingan dan perancangan aktiviti.

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
	Pelaksanaan EA di agensi sektor awam ialah berpandukan kepada Rangka kerja MyGovEA yang diadaptasi daripada *The Open Group Architecture Framework* (TOGAF).
Enkripsi *(Encryption)*	Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.
IaaS *(Infrastructure as a Service)*	Model perkhidmatan pengkomputeran awam yang menyediakan infrastruktur IT asas seperti pelayan maya, rangkaian, storan, dan sistem operasi secara atas talian. Pengguna mempunyai kawalan penuh terhadap infrastruktur ini tanpa perlu mengurus perkakasan fizikal.
ICT *(Information and Communication Technology)*	Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik.
ICTSO *(ICT Security Officer)*	Pegawai Keselamatan ICT, iaitu pegawai yang dilantik untuk bertanggungjawab terhadap keselamatan siber.
IDS *(Intrusion Detection System)*	Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem diceroboh. Terdapat dua bentuk IDS yang lazim, iaitu pengesanan salah guna dan pengesanan anomali. Dalam pengesanan salah guna, IDS menganalisis maklumat yang dikumpul dan membandingkannya dengan pangkalan data tandatangan serangan yang besar. Secara khusus IDS mencari serangan tertentu yang telah didokumenkan. Seperti sistem pengesan virus, keberkesanan perisian pengesan salah guna ini hanyalah bergantung kepada sebaik mana pangkalan data tandatangan serangan yang ada untuk membandingkan maklumat yang dikumpul.
Insiden Keselamatan Siber	Musibah *(adverse event)* yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar DKS sama ada yang ditetapkan secara tersurat atau tersirat.

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
Internet	Sistem rangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.
IPS *(Intrusion Prevention System)*	Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan seperti *malicious code*. Contoh: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
JDN	Jabatan Digital Negara (JDN) yang dulunya dikenali sebagai Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), iaitu sebuah agensi teknikal ICT dalam pemantapan tatakelola pelaksanaan inisiatif pendigitalan dan adaptasi teknologi digital baharu ke arah penyampaian perkhidmatan yang efisien, cerdas, selamat dan tangkas.
Jejak Audit *(Audit Trail)*	Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.
JMM	Jabatan Muzium Malaysia
JPICT	Merujuk kepada Jawatankuasa Pemandu ICT
JPM	Jabatan Perdana Menteri, iaitu sebuah kementerian kerajaan persekutuan Malaysia yang diketuai oleh Perdana Menteri Malaysia.
JPNIN	Jabatan Perpaduan Negara dan Integrasi Nasional
Kawasan Larangan	Kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja.
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
KPN/Agensi	Merujuk kepada Kementerian Perpaduan Negara dan Agensi dibawahnya.

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.
LAN *(Local Area Network)*	Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat.
Media Storan	Peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetik, *optical disk, flash disk*, CD ROM*, thumb drive* dan media storan lain.
NACSA *(National Cyber Security Agency)*	Agensi Keselamatan Siber Negara. Ditubuhkan pada Februari 2017 sebagai agensi negara yang menerajui hal ehwal keselamatan siber, dengan objektif memastikan keselamatan dan memperkukuhkan ketahanan Malaysia dalam menghadapi ancaman serangan siber, dengan mengkoordinasi dan mengkonsolidasi pakar-pakar dan sumber negara dalam bidang keselamatan siber.
Outsource	Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi tertentu bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui.
PaaS (*Platform as a Service*)	Platform pembangunan (seperti pelayan, pangkalan data, dan alat pembangunan) untuk pembangun membina, menguji dan melancarkan aplikasi seperti Google App Engine, Heroku, Microsoft Azure App Services.
Pembekal	Individu, entiti perniagaan atau organisasi yang menyediakan produk atau perkhidmatan kepada Pengguna.
Pemegang Taruh	Semua pihak yang mempunyai kepentingan dengan Kementerian dan Agensi.
Pemilik Sistem	Pemilik bisnes *(business owner)* bagi sistem yang dibangunkan atau Bahagian/Unit/Institut/Tribunal/Agensi/Jabatan di bawah KPN/Agensi yang paling banyak memiliki data dalam sesuatu sistem.
Pengguna	Warga Cawangan/Bahagian/Unit/Agensi di bawah KPN/Agensi termasuk pegawai yang berkhidmat

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
	secara kontrak atau pegawai khidmat singkat yang menggunakan aset ICT dan siber secara langsung atau tidak langsung.
Pengurusan Fasiliti	Proses penyelenggaraan, pengurusan, dan pengoperasian kemudahan fizikal sesebuah organisasi bagi memastikan persekitaran kerja yang selamat, cekap, dan berfungsi dengan baik. Ini merangkumi pengurusan bangunan, peralatan, utiliti, keselamatan, serta kebersihan.
Pentadbir Pangkalan Data	Pentadbir yang menguruskan dan menyelenggarakan pangkalan data.
Pentadbir Pusat Data	Pentadbir yang menguruskan dan menyelenggarakan Pusat Data
Pentadbir Rangkaian	Pentadbir yang menguruskan dan menyelenggarakan rangkaian dan keselamatan
Pentadbir Server	Pentadbir yang mengurus server fizikal dan virtual
Pentadbir Sistem Aplikasi	Pentadbir yang membangunkan, melaksanakan dan menyelenggara sistem aplikasi, laman web, media sosial dan aplikasi mudah alih.
Peralatan ICT	Merujuk kepada perkakasan dan perisian ICT.
Peralatan Mudah Alih	Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti *tablet*, *Personal Digital Assistant* (PDA), telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu *Universal Serial Bus* (USB) dan sebagainya.
Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contoh: *Linux* dan *Windows*), sistem utiliti (contoh: *Disk Cleanup* dan *Disk Defragmenter*) dan perisian aplikasi (contoh: *Microsoft Office* dan *Google Chrome*).
Perkakasan ICT	Merujuk kepada komponen dalaman peralatan ICT.
Pihak Ketiga	Pakar runding, syarikat dan individu yang mempunyai urusan dengan perkhidmatan ICT dan siber serta dilantik untuk melaksanakan tugas di KPN/Agensi dalam jangka masa yang tertentu.

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
PII *(Personal Identifiable Information)*	Maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu.
PKI *(Public Key Infrastructure)*	Infrastruktur Kunci Awam, iaitu sistem enkripsi lengkap khusus untuk mencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
PKP	Pengurusan Kesinambungan Perkhidmatan *(Business Continuity Management)*, bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama agensi dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana.
PKS	Polisi Keselamatan Siber, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT dan ruang siber.
PKS KPN	Merujuk kepada Dokumen Polisi Keselamatan Siber Kementerian Perpaduan Negara dan Agensi dibawahnya
PNM	Perpustakaan Negara Malaysia
RC	*Recover*
Restore	Aktiviti pemulihan atau penyalinan semula data daripada media penduaan.
Router	Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. contoh: capaian Internet.
RP	*Respond*
RPO (*Recovery Point Objective)*	Objektif Titik Pemulihan
RTO (*Recovery Time Objective)*	Objektif Masa Pemulihan (RTO)

AKRONIM/TERMA/TAKRIFAN	KETERANGAN
SaaS *(Software as a Service)*	Model perkhidmatan pengkomputeran awam yang membolehkan pengguna mengakses perisian melalui internet tanpa perlu memasang (*installation*) atau menyelenggara (*maintenance*) perisian tersebut. Semua infrastruktur dikendalikan oleh penyedia perkhidmatan seperti Gmail, Microsoft 365, Google Docs, Zoom.
Server	Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lain yang mempunyai hubungan rangkaian dengannya.
Siber	Ruang maya yang diwujudkan oleh rangkaian komputer sejagat. Ruang tempat berlangsungnya kegiatan pemanfaatan ICT dan internet ini disebut ruang siber. Ruang siber *(cyberspace)* atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya internet) untuk melakukan pelbagai kegiatan sehari-hari.
Sistem ICT	Merangkumi Sistem Aplikasi, Sistem Pusat Data, Rangkaian dan Komunikasi ICT.
SLA *(Service Level Assurance)*	Perjanjian Tahap Perkhidmatan, iaitu komponen kontrak perkhidmatan antara pembekal perkhidmatan dan pelanggan. SLA menyediakan aspek khusus dan terukur yang berkaitan dengan penawaran perkhidmatan.
Switch	Alat yang boleh menapis *(filter)* dan memajukan *(forward)* isyarat paket data antara segmen rangkaian LAN.
UC *(Unified Communication)*	Saluran-saluran komunikasi elektronik selain e-mel yang disepadukan dalam satu rangkaian dan antara muka yang sama.
UPS *(Uninterruptible Power Supply)*	Satu alat yang akan membekalkan kuasa secara automatik kepada peralatan komputer khususnya dan peralatan elektrik umumnya apabila bekalan elektrik utama terputus.
WAN *(Wide Area Network)*	Rangkaian komunikasi yang merangkumi kawasan geografi yang luas di seluruh bandar, negara atau rantau.

MAKLUMAT DAN KETERANGAN DOKUMEN

Polisi Keselamatan Siber (PKS) merupakan satu set garis panduan dan prosedur rasmi yang dirangka khusus bagi melindungi aset digital, maklumat, dan infrastruktur teknologi maklumat dan komunikasi (ICT) milik KPN/Agensi daripada sebarang ancaman siber.

PKS menetapkan peraturan, tatacara, dan kawalan keselamatan yang wajib dipatuhi oleh semua pihak yang berkepentingan, termasuk warga kerja, penyedia perkhidmatan dan pihak ketiga, bagi memastikan keselamatan rangkaian, sistem, dan data KPN/Agensi sentiasa terpelihara daripada akses tanpa kebenaran, pencerobohan, kebocoran maklumat, atau serangan siber.

Polisi ini merangkumi aspek seperti penilaian risiko, pengurusan kelemahan keselamatan, perlindungan data dan maklumat, pengurusan keistimewaan pengguna, pematuhan terhadap undang-undang dan peraturan yang berkuatkuasa, serta tatacara tindak balas terhadap insiden keselamatan siber.

PKS berfungsi sebagai rangka kerja keselamatan yang menyeluruh bagi memastikan kerahsiaan, integriti dan ketersediaan sistem serta maklumat kritikal organisasi sentiasa dilindungi dan diurus secara sistematik mengikut amalan terbaik keselamatan maklumat.

ISI KANDUNGAN

1 PENGENALAN

1.1 Pengenalan

Memastikan polisi keselamatan maklumat bersesuaian, berterusan dan seiring dengan hala tuju pengurusan dalam menyokong keselamatan maklumat selari dengan fungsi, undang-undang dan keperluan kontrak perjanjian.

Polisi Keselamatan Siber (PKS) Kementerian Perpaduan Negara (KPN) bersama Agensi di bawahnya menetapkan peraturan yang wajib dipatuhi oleh semua pengguna dalam penggunaan sumber teknologi maklumat dan komunikasi (ICT) milik Kementerian dan Agensi. Polisi ini menghuraikan pendekatan keselamatan ICT yang diguna pakai serta menjelaskan tanggungjawab dan peranan setiap pengguna dalam memastikan keselamatan, integriti dan kerahsiaan aset ICT KPN dan Agensi sentiasa terpelihara.

1.2 Tujuan

Polisi ini bertujuan untuk menjelaskan peranan, tanggungjawab, arahan, peraturan, garis panduan dan amalan yang **MESTI DIBACA, DIFAHAMI** dan **DIPATUHI** oleh semua warga, pembekal, pakar runding serta pihak lain yang terlibat dengan perkhidmatan ICT. Dokumen ini berfungsi sebagai panduan utama dalam usaha melindungi maklumat dan data sensitif dalam ruang siber.

1.3 Objektif

Polisi ini diwujudkan bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi KPN dan Agensi. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Objektif utama PKS KPN dan Agensi ialah seperti berikut:

a. Memastikan kelancaran operasi KPN/Agensi dan meminimumkan kerosakan atau kemusnahan;
b. Melindungi kepentingan 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;
e. Memastikan pemantauan berterusan ke atas perkhidmatan keselamatan ICT KPN/Agensi ;
f. Melaksanakan analisis ke atas sumber ICT KPN dan Agensi ; dan
g. Melaksanakan sistem pengurusan keselamatan maklumat di KPN dan Agensi.

1.4 Skop

Polisi ini merupakan dokumen rujukan induk yang diguna pakai secara menyeluruh oleh Kementerian Perpaduan Negara dan Agensi. Dokumen ini merangkumi semua aset maklumat dan sistem ICT yang digunakan oleh KPN/Agensi tanpa pengecualian. Aset-aset ini termasuk data dan maklumat, perkakasan, perisian, infrastruktur ICT, individu dan premis. Kesemua aset ini amat penting dalam menyokong urusan rasmi kerajaan yang melibatkan masyarakat, sektor swasta dan Agensi kerajaan lain.

a. Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

b. semua data dan maklumat hendaklah 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, Polisi Keselamatan Siber 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 pengendalian meliputi perkara berikut:

a. Data atau Maklumat
Merangkumi semua bentuk data sama ada digital (*softcopy*) atau bercetak (*hardcopy*) yang digunakan bagi menyokong misi dan objektif KPN/Agensi, termasuk dokumentasi, prosedur operasi, rekod, profil pelanggan, pangkalan data, fail data dan maklumat arkib.

b. Salinan Digital *(Softcopy)*
Koleksi fakta-fakta dalam digital atau elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif. (Contohnya: Rekod-rekod digital, profil pelanggan, pangkalan data dan fail-fail data, maklumat arkib dan lain-lain);

c. Salinan Bercetak *(Hardcopy)*
Koleksi fakta-fakta dalam bentuk kertas atau bercetak, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif. (Contohnya: Sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, fail-fail dan lain-lain);

d. Perkakasan *(Hardware)*

Semua aset fizikal yang digunakan untuk pemprosesan maklumat dan kemudahan storan, seperti komputer, pelayan (server) dan peralatan komunikasi.

e. Perisian (software)

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam 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 KPN/Agensi ;

f. Infrastruktur ICT

Merujuk kepada set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang membolehkan penghantaran, penyimpanan, pemprosesan dan mendapatkan semula maklumat dalam organisasi atau merentasi pelbagai organisasi. Ia termasuk sistem komputer, Server, pangkalan data, rangkaian (kedua-dua kawasan tempatan dan luas), sambungan internet, sistem komunikasi, pusat data, perkhidmatan pengkomputeran awan *(cloud computing)* dan peralatan dan teknologi lain yang diperlukan. Infrastruktur ICT yang direka bentuk dan dilaksanakan untuk menyokong dan membolehkan pelbagai jenis perkhidmatan dan aplikasi teknologi maklumat dan komunikasi berfungsi bagi mencapai objektif dan misi yang ditetapkan. Infrastruktur ICT ini termasuk:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses;
iii. Perkhidmatan pengkomputeran awam (SaaS/PaaS/IaaS): dan
iv. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

g. Manusia

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

h. Premis

Semua kemudahan serta premis yang menempatkan aset ICT, termasuk bilik komputer, pusat data, bangunan KPN/Agensi atau mana-mana premis kerajaan atau swasta yang digunakan untuk menempatkan perkara a hingga h di atas.

1.5 Pernyataan Polisi

Aset maklumat merupakan aset kritikal dan bernilai yang perlu dilindungi dengan sewajarnya. Keselamatan aset maklumat ditakrifkan sebagai satu keadaan yang bebas daripada sebarang ancaman atau risiko yang tidak boleh diterima. Penjagaan keselamatan maklumat merupakan satu proses yang berterusan dan melibatkan pelaksanaan aktiviti berkala dari semasa ke semasa bagi memastikan aset sentiasa dilindungi, memandangkan ancaman dan kelemahan siber sentiasa berubah.
Perlindungan aset maklumat ini merangkumi semua bentuk maklumat dan data elektronik yang diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dihantar serta disalin. Langkah perlindungan ini bertujuan untuk menjamin keselamatan aset maklumat dalam ruang siber dengan memastikan aspek kerahsiaan, integriti, kebolehsahan *(validity),* kesahihan dan ketersediaan hanya dapat dicapai oleh pengguna yang diberi kebenaran.

Penjelasan ciri-ciri utama keselamatan aset maklumat yang perlu dijaga adalah seperti berikut:

a. **Kerahsiaan –** Maklumat tidak boleh didedahkan atau diakses tanpa kebenaran pihak yang diberi kuasa.

b. **Integriti –** Data dan maklumat mestilah tepat, lengkap dan sentiasa dikemaskini. Sebarang pindaan hanya boleh dibuat melalui kaedah yang dibenarkan.

c. **Kebolehsahan** *(validity)* **–** Sumber data dan maklumat hendaklah dapat dibuktikan sah dan tidak boleh dinafikan oleh pihak yang menghasilkannya.

d. **Kesahihan –** Data dan maklumat mestilah sah dan diperoleh daripada sumber yang boleh dipercayai.

e. **Ketersediaan –** Data dan maklumat hendaklah sentiasa boleh diakses apabila diperlukan.

Langkah-langkah untuk memelihara keselamatan aset maklumat perlu bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa, kelemahan sistem ICT, serta ancaman yang timbul daripada kelemahan tersebut. Risiko yang dikenal pasti perlu ditangani melalui langkah pencegahan yang sewajarnya.

Penetapan kawalan keselamatan yang sesuai hendaklah berdasarkan klasifikasi data dan maklumat, serta nilai atau kepentingan aset maklumat. Klasifikasi ini hendaklah berpandukan kepada arahan, pekeliling atau garis panduan kerajaan yang berkuatkuasa.

Keselamatan aset maklumat merupakan tanggungjawab bersama semua warga KPN/ Agensi dan pihak ketiga yang berurusan dengan perkhidmatan ICT KPN/Agensi.

1.6 Prinsip Keselamatan

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber KPN/Agensi yang perlu dipatuhi adalah seperti berikut:

a. Akses Atas Dasar Perlu Mengetahui

Akses kepada aset maklumat hanya diberikan untuk tujuan tertentu dan dihadkan kepada pengguna yang memerlukan, berdasarkan prinsip "perlu mengetahui". Ini bermaksud akses hanya dibenarkan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut bagi melaksanakan tugas rasmi.

b. Hak Akses Minimum

Pengguna hendaklah diberikan hak akses minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja.

c. Akauntabiliti

Setiap pengguna adalah bertanggungjawab sepenuhnya terhadap segala tindakan yang dilakukan ke atas aset maklumat KPN/Agensi . Tanggungjawab ini hendaklah dinyatakan secara jelas dan bersesuaian dengan tahap sensitiviti setiap sumber atau aset maklumat yang diuruskan.

Bagi memastikan tanggungjawab tersebut dapat dikuatkuasakan, sistem ICT hendaklah dilengkapi dengan keupayaan untuk mengesan dan mengesahkan aktiviti pengguna, bagi membolehkan setiap tindakan dipertanggungjawabkan kepada individu yang melaksanakannya. Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d. Pengasingan Tugas

Bagi mengekalkan prinsip semak dan imbang *(check and balance)*, KPN serta semua Agensi di bawah seliaannya, hendaklah melaksanakan pengasingan tugas bagi semua fungsi yang bersifat kritikal.

Tugas-tugas penting tidak boleh dilaksanakan sepenuhnya oleh seorang pengguna sahaja yang bertindak secara bersendirian tanpa semakan atau pengesahan oleh pihak lain.

Fungsi seperti mewujudkan, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan antara pengguna bagi mengelakkan akses tanpa kebenaran, serta bagi melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau sebarang bentuk manipulasi.

Pengasingan tugas ini turut merangkumi pemisahan antara kumpulan operasi, rangkaian, keselamatan dan aplikasi, bergantung kepada keperluan dan struktur organisasi di bawah KPN/Agensi .

e. Prinsip Amanah Sifar *(zero trust)*

Konsep keselamatan ini bertujuan untuk memperkukuh postur keselamatan keseluruhan dengan mengamalkan pendekatan yang menganggap setiap peranti dan pengguna sama ada berada di dalam atau di luar perimeter rangkaian sebagai entiti yang berpotensi terjejas. Oleh itu, tiada entiti diberi kepercayaan secara automatik. Setiap permintaan untuk capaian rangkaian mesti disahkan seolah-olah ia datang daripada rangkaian terbuka dan tidak selamat. Prinsip-prinsip asas pendekatan Amanah Sifar adalah seperti berikut:

i. Semua trafik rangkaian (dalaman dan luaran) dianggap tidak dipercayai – Tiada perbezaan antara akses dari dalam atau luar; semua perlu disahkan terlebih dahulu.
ii. Akses kepada sumber diberikan berdasarkan penilaian menyeluruh – Ini termasuk identiti pengguna, status keselamatan peranti, lokasi dan faktor kontekstual lain yang relevan. Akses hanya dibenarkan selepas pengesahan berjaya dilakukan.
iii. Prinsip keistimewaan minimum dikuatkuasakan – Pengguna hanya diberikan akses kepada sumber yang diperlukan, pada masa yang diperlukan, dan untuk tempoh yang minimum sahaja.

f. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, Server, router, firewall dan peralatan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan

keselamatan *(audit trail);*

g. Pematuhan

Polisi Keselamatan Maklumat KPN/Agensi hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat;

h. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kesediaan 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

i. Saling Bergantungan

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

1.7 Ciri Keselamatan Data Dan Maklumat

Aset maklumat merupakan aset kritikal dan bernilai yang perlu dilindungi dengan sewajarnya. Keselamatan aset maklumat ditakrifkan sebagai satu keadaan yang bebas daripada sebarang ancaman atau risiko yang tidak boleh diterima. Penjagaan keselamatan maklumat merupakan satu proses yang berterusan dan melibatkan pelaksanaan aktiviti berkala dari semasa ke semasa bagi memastikan aset sentiasa dilindungi, memandangkan ancaman dan kelemahan keselamatan siber sentiasa berubah.

a. **Kerahsiaan**

Kerahsiaan merujuk kepada perlindungan maklumat daripada capaian yang tidak dibenarkan. Ciri keselamatan ini bertujuan untuk memastikan bahawa hanya pihak yang sah dan berhak sahaja boleh mencapai maklumat tertentu. Perkara ini penting untuk melindungi maklumat sensitif seperti data peribadi, maklumat kewangan dan rahsia perniagaan. Langkah-langkah yang biasa digunakan untuk mengekalkan kerahsiaan termasuk penyulitan maklumat, kawalan capaian yang ketat dan penggunaan kata laluan yang kukuh.

b. **Integriti**

Integriti merujuk kepada ketepatan, kelengkapan dan kesempurnaan maklumat. Ciri ini diperlukan bagi memastikan bahawa data dan maklumat tidak diubah suai atau dirosakkan oleh pihak yang tidak dibenarkan. Sebarang perubahan terhadap data atau maklumat hendaklah dilakukan hanya oleh

pihak yang mempunyai kebenaran yang sah dan perubahan tersebut haruslah direkodkan dengan jelas untuk tujuan audit. Integriti adalah sangat penting dalam memastikan bahawa keputusan yang dibuat berdasarkan maklumat tersebut adalah tepat dan boleh dipercayai.

c. **Tidak Boleh Disangkal**
Ciri ini memastikan bahawa pihak yang bertanggungjawab terhadap penciptaan, penghantaran, penerimaan data atau maklumat tidak boleh dinafikan penglibatan mereka. Dalam transaksi digital, ciri ini dapat membuktikan penglibatan pihak tertentu dalam transaksi secara digital yang dilaksanakan. Contoh langkah keselamatan yang digunakan untuk memastikan tiada penafian adalah termasuk penggunaan tandatangan digital dan rekod transaksi yang terperinci dalam jejak audit.

d. **Kesahihan**
Kesahihan merujuk kepada pengesahan bahawa data dan maklumat adalah sah dan berasal daripada sumber yang dipercayai. Ciri kesahihan memastikan bahawa maklumat yang diterima atau dihantar tidak dimanipulasi oleh pihak ketiga. Langkah-langkah seperti penggunaan sijil digital dan protokol pengesahan membantu memastikan bahawa maklumat yang diterima adalah sahih dan boleh dipercayai.

e. **Ketersediaan**
Ketersediaan memastikan bahawa maklumat boleh dicapai oleh pihak yang dibenarkan pada bila-bila masa yang diperlukan. Ketersediaan adalah penting untuk memastikan kelancaran operasi harian dan membuat keputusan yang tepat pada masanya. Untuk mengekalkan ketersediaan, semua pihak yang terlibat hendaklah melaksanakan langkah-langkah seperti menyediakan dan mengaktifkan pelan pemulihan bencana, menyediakan sistem sandaran dan melaksanakan pengurusan risiko yang menyeluruh untuk mengurangkan gangguan terhadap capaian data dan maklumat.

1.8 Implikasi Ketidakpatuhan

Ketidakpatuhan terhadap PKS akan menjejaskan pengurusan dan memberi implikasi seperti di bawah:

a. Risiko Keselamatan Maklumat iaitu kelemahan dalam pelaksanaan polisi keselamatan maklumat yang akan meningkatkan risiko kehilangan, kebocoran atau pengubahsuaian maklumat yang penting dan sensitif.

b. Pelanggaran Undang-undang dan Peraturan iaitu tidak mematuhi piawaian keselamatan maklumat. Ini boleh dikenakan tindakan undang-undang, denda atau lain-lain peraturan yang berkuatkuasa.

c. Kehilangan Kepercayaan Awam dan Pemegang Taruh sekiranya Warga KPN/Agensi tidak menjaga keselamatan maklumat dengan baik dan akan memberi kesan negatif terhadap reputasi organisasi.

1.9 Pemakaian

Polisi ini terpakai kepada semua warga KPN mahupun Agensi serta pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT di KPN/Agensi.

1.10 Pembatalan

Dengan berkuatkuasanya PKS ini, maka Polisi Keselamatan Siber versi 1.0 adalah dibatalkan.

2 TADBIR URUS

2.1 Tadbir Urus

Bagi memastikan pelaksanaan Polisi Keselamatan Siber (PKS) berjalan dengan berkesan dan mencapai objektif, struktur tadbir urus Jawatankuasa Pemandu ICT (JPICT) ditetapkan selaras dengan Surat Pekeliling Am Bilangan 7 Tahun 2024, Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam yang telah dikeluarkan oleh Jabatan Perdana Menteri pada 16 Julai 2024 atau arahan semasa Kerajaan Malaysia.

Keahlian Jawatankuasa Kementerian ini adalah seperti berikut;

Pengerusi:	Ketua Setiausaha Kementerian atau Pegawai yang diturunkan kuasa
Ahli Tetap:	Ketua Bahagian di bawah Kementerian Ketua Pegawai Digital (CDO) Kementerian Pengurus ICT Kementerian/Agensi Ketua Agensi atau Ketua Pegawai Digital (CDO) Agensi Ketua Pegawai Keselamatan ICT (ICTSO) Kementerian
Ahli Jemputan:	Ahli-ahli jemputan yang berkaitan
Urusetia:	Bahagian/Unit/Seksyen ICT Kementerian
Terma rujukan:	i. Menetapkan hala tuju dan strategi untuk pembangunan dan pelaksanaan projek ICT Kementerian; ii. Mengesahkan cadangan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan projek ICT Kementerian dan semua Agensi di bawahnya; iii. Merancang, menyelaras dan menyeragamkan pembangunan dan pelaksanaan projek ICT Kementerian dan semua Agensi di bawahnya supaya selaras dengan pelan strategik organisasi, Pelan Strategik Pendigitalan Kementerian/Agensi, Pelan Strategik Pendigitalan Sektor Awam (PSPSA) atau pelan yang setara; iv. Menilai dan melulus semua cadangan perolehan ICT Kementerian dan Agensi di bawahnya berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;

	v. Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi kementerian dan semua Agensi di bawahnya kepada JTISA vi. untuk kelulusan teknikal berdasarkan had nilai yang ditetapkan; vii. Memastikan pelaksanaan projek ICT dipantau dan dilaporkan melalui sistem yang disediakan oleh JDN; viii. Mempromosi dan menggalakkan perkongsian pintar aplikasi ICT antara Kementerian dan semua Agensi di bawahnya; ix. Meluluskan dasar/aktiviti keselamatan ICT Kementerian dan Agensi di bawahnya; x. Memastikan keselarasan projek ICT agar tiada duplikasi dan pembaziran.
Kehadiran Mesyuarat:	Mesyuarat boleh dilaksanakan dengan kehadiran 2/3 daripada jumlah ahli mesyuarat.

Keahlian Jawatankuasa Agensi ini adalah seperti berikut;

Pengerusi:	Ketua Jabatan atau Pegawai Yang Diberi Kuasa
Pengerusi Ganti:	Timbalan Ketua Jabatan
Ahli Tetap:	Ketua Pegawai Digital (CDO) atau yang setara Ketua Bahagian Pengurus ICT Ketua Pegawai Keselamatan ICT (ICTSO) Ahli-ahli lain yang dilantik tetap
Ahli Jemputan:	Ahli-ahli jemputan yang berkaitan
Urusetia:	Bahagian/Unit/Seksyen ICT Kementerian
Terma rujukan:	i. Menetapkan hala tuju dan strategi untuk pembangunan dan pelaksanaan projek ICT Agensi; ii. Mengesahkan cadangan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan projek ICT agensi; iii. Merancang, menyelaras dan menyeragamkan pembangunan dan pelaksanaan projek ICT Agensi supaya selaras dengan pelan strategik organisasi, Pelan Strategik

	Pendigitalan Agensi, Pelan Strategik Pendigitalan Sektor Awam (PSPSA) atau pelan yang setara; iv. Menilai dan melulus semua cadangan perolehan ICT agensi berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan - peraturan semasa yang berkaitan; v. Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi agensi kepada JPICT Kementerian untuk kelulusan teknikal berdasarkan had nilai yang ditetapkan; vi. Memastikan pelaksanaan projek dipantau dan dilaporkan melalui sistem yang disediakan oleh JDN; vii. Mempromosi dan menggalakkan perkongsian pintar aplikasi ICT agensi; viii. Meluluskan dasar/aktiviti keselamatan ICT agensi; ix. Memastikan keselarasan projek ICT agar tiada duplikasi dan pembaziran
Kehadiran Mesyuarat:	Mesyuarat boleh dilaksanakan dengan kehadiran 2/3 daripada jumlah ahli mesyuarat.

3 PENGURUSAN RISIKO

3.1 Pengurusan Risiko

Semua pihak yang terlibat dalam pengurusan data dan maklumat di KPN serta Agensi di bawahnya hendaklah mengambil kira risiko yang wujud terhadap aset maklumat, khususnya yang berpunca daripada kelemahan (*vulnerability*) dan ancaman yang semakin kompleks dalam persekitaran digital masa kini.

Oleh itu, langkah-langkah proaktif dan bersesuaian perlu diambil bagi menilai tahap risiko ke atas aset maklumat, bagi memastikan pendekatan dan tindakan perlindungan yang paling berkesan dapat dikenalpasti dan dilaksanakan. Penilaian risiko ini bertujuan untuk:

a. Mengenal pasti risiko terhadap keselamatan maklumat;
b. Menentukan tindakan susulan dan langkah mitigasi yang sesuai; dan
c. Mengurangkan atau mengawal tahap risiko berdasarkan hasil penilaian.

Penilaian risiko keselamatan maklumat hendaklah dilaksanakan secara berkala, sekurang-kurangnya sekali setahun, atau apabila berlaku perubahan ke atas aset maklumat.

Laporan Penilaian Risiko dan Pelan Penguraian Risiko hendaklah dijadikan agenda tetap dalam mesyuarat bahagian atau mesyuarat setara dan dibincangkan secara menyeluruh serta dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ICT KPN/Agensi. Penilaian risiko hendaklah merangkumi semua aset maklumat termasuk:

a. Aset fizikal (contoh: Server, peralatan storan, peranti rangkaian);
b. Aplikasi, sistem dan perisian;
c. Proses dan prosedur yang berkaitan; serta
d. Premis yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utiliti, dan sistem sokongan lain.

3.2 Pelaksanaan Pengurusan Risiko

Pelaksanaan pengurusan risiko keselamatan maklumat hendaklah selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024.

Dalam menghadapi potensi risiko, semua pihak yang terlibat hendaklah mengenal pasti tindakan yang sewajarnya, termasuk:

a. Mengurangkan risiko melalui pelaksanaan kawalan keselamatan yang bersesuaian;
b. Menerima atau bersedia menghadapi risiko yang tidak dapat dielakkan selagi ia tidak menjejaskan penyampaian perkhidmatan KPN/Agensi ;
c. Mengelakkan risiko dengan melaksanakan langkah-langkah pencegahan yang

boleh menghalang risiko daripada berlaku; dan

d. Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding atau pihak berkepentingan lain melalui perjanjian dan kontrak yang sesuai

4 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

4.1 Pelan Pengurusan Keselamatan maklumat

Setiap projek di KPN mahupun Agensi hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan kursus yang lain.

Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKS dan surat pekeliling/ arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan.

Pelan ini hendaklah mengenal pasti pelindung mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen yang berikut:

a. **Peranti Pengkomputeran Peribadi**
   Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, telefon pintar, tablet dan peranti storan.

b. **Peranti Rangkaian**
   i. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti switch, penghala rangkaian, tembok keselamatan, peranti Virtual Private Network (VPN) dan kabel.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

c. **Aplikasi**
   i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah Server web, Server aplikasi dan sistem operasi.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam penggunaan, data-dalam-pergerakan, data dalam simpanan dan
   iii. menghalang ketirisan data hendaklah diperincikan dalam Pelan

Pengurusan Keselamatan Maklumat.

d. **Server**
   i. Server merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Server hendaklah diletakkan di lokasi yang selamat.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

e. **Persekitaran Fizikal**
   i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.
   ii. Keselamatan Kerajaan untuk mendapatkan nasihat serta hendaklah selaras dengan perundangan dan arahan yang sedang berkuat kuasa.
   iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan defense-in-depth.
   iv. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5 KAWALAN ORGANISASI

5.1 Kawalan Organisasi

Terdapat kawalan organisasi yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di Kementerian Perpaduan Negara dan Agensi di bawahnya. Perincian kawalan organisasi seperti di bawah.

ID	PENERANGAN	PERANAN
5.1.1	**Pelaksanaan Polisi** Pelaksanaan polisi ini akan diketuai oleh Ketua Setiausaha (KSU) / Ketua Agensi dan dipantau melalui dalam Mesyuarat JPICT dan dan disokong oleh Jawatankuasa Pemandu ICT.	Ketua Setiausaha / Ketua Agensi, JPICT, CSIRT, ICTSO, CDO
5.1.2	**Pengesahan Polisi** Polisi Keselamatan Siber ini telah disemak, disahkan, dan diluluskan oleh pihak pengurusan tertinggi KPN/Agensi . Pengesahan ini menandakan komitmen penuh pihak pengurusan dalam memastikan pematuhan terhadap polisi serta pelaksanaan kawalan keselamatan maklumat secara menyeluruh dan berterusan di seluruh KPN dan Agensi di bawahnya. Segala pindaan atau semakan terhadap polisi ini hendaklah mendapat kelulusan rasmi daripada Ketua Setiausaha (KSU)/Ketua Agensi dan akan diselaraskan melalui Jawatankuasa Pemandu ICT (JPICT) untuk memastikan keseragaman serta keberkesanan pelaksanaannya.	Ketua Setiausaha (KSU) / Ketua Agensi
5.1.3	**Penguatkuasaan Polisi** Polisi Keselamatan Siber Kementerian Perpaduan Negara dan Agensi hendaklah dipatuhi oleh semua warga Kementerian/Agensi, pembekal, pakar runding serta mana-mana pihak yang mempunyai urusan berkaitan perkhidmatan ICT di KPN/Agensi.	Pemegang Taruh

ID	PENERANGAN	PERANAN
	Sebarang ketidakpatuhan terhadap dasar ini boleh dikenakan tindakan tatatertib dan/atau apa-apa remedi serta tindakan undang-undang lain yang diperuntukkan di bawah akta, peraturan atau undang-undang semasa yang berkuat kuasa. Sebarang ketidakpatuhan terhadap polisi ini boleh dikenakan tindakan tatatertib, dan/atau sebarang remedi serta tindakan undang-undang berdasarkan akta, peraturan atau undang-undang yang berkuatkuasa. Piawaian dan prosedur berkaitan yang ditetapkan dalam dokumen ini juga hendaklah dipatuhi sepenuhnya oleh semua pihak yang terlibat.	
5.1.4	**Penyebaran Polisi** Program kesedaran mengenai polisi ini hendaklah dirancang dan diselaraskan dengan rapi, di samping memastikan dasar ini disebarkan secara menyeluruh dan dipatuhi oleh semua pengguna aset ICT serta pihak ketiga yang berurusan atau menyediakan perkhidmatan ICT kepada KPN/Agensi.	ICTSO, dan Pasukan Keselamatan Digital ICTSO
5.1.5	**Pengecualian Polisi** Keselamatan ICT Kementerian terpakai kepada warga KPN dan Agensi dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidmatan ICT di KPN /Agensi dan tiada pengecualian diberikan	Semua Pemegang Taruh yang terlibat
5.1.6	**Penyelenggaraan Polisi** Penyelenggaraan dan kajian semula dasar perlu disemak sekurang-kurangnya tiga tahun sekali atau mengikut keperluan semasa atau apabila diperlukan. Semua dokumen dan rekod hendaklah diwujudkan serta diselenggara dengan teratur bagi membuktikan pematuhan terhadap	ICTSO, CSIRT, Pasukan Keselamatan Digital KPN/Agensi

ID	PENERANGAN	PERANAN
	keperluan serta memastikan keberkesanan operasi pengurusan keselamatan maklumat. Dokumen dan rekod tersebut juga hendaklah dilindungi serta dikawal selaras dengan undang-undang, arahan, peraturan dan garis panduan semasa yang berkuat kuasa.	
5.1.7	**Kajian Semula/Semakan Polisi** Polisi ini perlu disemak dan dipinda secara berkala mengikut tempoh yang ditetapkan, atau apabila berlaku perubahan dalam teknologi ICT, prosedur, perundangan, atau dasar kerajaan. Tujuan semakan ini adalah untuk memastikan polisi sentiasa relevan, mencukupi dan berkesan. a. Memastikan pelaksanaan dan pematuhan terhadap polisi sentiasa dipantau dan dikuatkuasakan. b. Ketua Bahagian bertanggungjawab mengenal pasti dan mencadangkan sebarang pindaan yang diperlukan. c. Cadangan pindaan hendaklah dikemukakan secara bertulis kepada ICTSO untuk semakan awal dan dibawa ke JPICT untuk pengesahan. d. Pindaan yang telah disahkan oleh JPICT perlu dimaklumkan kepada semua pengguna dan pihak ketiga.	Ketua Bahagian, ICTSO, JPICT KPN/Agensi

5.2 Peranan dan Tanggungjawab Keselamatan Maklumat

Menjelaskan secara teratur peranan dan tanggungjawab setiap individu yang terlibat, bagi memastikan pelaksanaan polisi keselamatan maklumat berjalan lancar dan mencapai matlamat yang ditetapkan.

ID	PENERANGAN	PERANAN
5.2.1	**Ketua Setiausaha (KSU)/ Ketua Pengarah** Peranan dan tanggungjawab Ketua Setiausaha (KSU) / Ketua Pengarah adalah seperti berikut: a. Memastikan penguatkuasaan Polisi Keselamatan Maklumat dilaksanakan secara berkesan. b. Memastikan semua pengguna termasuk pihak ketiga memahami dan mematuhi peruntukan yang ditetapkan dalam polisi. c. Memastikan keperluan sumber seperti kewangan, personel dan perlindungan keselamatan ICT adalah mencukupi untuk menyokong pelaksanaan polisi. d. Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan mengikut garis panduan yang sedang berkuatkuasa. e. Melantik CDO dan ICTSO di KPN/Agensi bagi menyokong pelaksanaan dan pemantauan keselamatan maklumat.	Ketua Setiausaha/ Ketua Pengarah
5.2.2	**Ketua Pegawai Digital (CDO)** Peranan dan tanggungjawab CDO adalah seperti berikut: Membantu Ketua Setiausaha / Ketua Pengarah dalam melaksanakan tugas-tugas berkaitan keselamatan siber seperti yang digariskan dalam polisi ini. Memastikan kawalan keselamatan maklumat diseragamkan dan diselaraskan di seluruh organisasi. Memastikan Pelan Strategik Pendigitalan	CDO

ID	PENERANGAN	PERANAN
	merangkumi elemen keselamatan siber secara menyeluruh. Menyelaras pelaksanaan pelan latihan dan program kesedaran berkaitan keselamatan siber bagi meningkatkan tahap pemahaman dan pematuhan pengguna.	
5.2.3	**Pegawai Keselamatan ICT (ICTSO)** Peranan dan tanggungjawab ICTSO adalah seperti berikut: a. **Dasar dan Prosedur** i. Mewujudkan garis panduan, prosedur dan tatacara keselamatan ICT yang selaras dengan keperluan polisi ini. ii. Merangka pelan pengurusan risiko dan audit keselamatan siber berdasarkan rangka kerja, polisi, pekeliling, garis panduan dan pelan pengurusan keselamatan maklumat yang berkuat kuasa. **b. Amaran dan Nasihat Keselamatan** i. Menyediakan dan menyebarkan amaran berkaitan potensi ancaman keselamatan siber. ii. Memberi khidmat nasihat dan mencadangkan langkah perlindungan yang bersesuaian bagi menangani risiko yang dikenalpasti. **c. Pengurusan Insiden** i. Melaporkan insiden keselamatan siber kepada CSIRT KPN/Agensi dan membantu dalam proses penyiasatan serta pemulihan. ii. Melaporkan insiden kepada CIO/CDO sekiranya melibatkan keperluan untuk Pengurusan	ICTSO

ID	PENERANGAN	PERANAN
	Kesinambungan Perkhidmatan (PKP). iii. Bekerjasama dengan pihak berkaitan dalam mengenal pasti punca insiden dan memperakukan tindakan pemulihan segera. **d. Pematuhan Polisi** i. Memastikan semua pengguna, dan pihak ketiga yang berurusan dengan perkhidmatan ICT mematuhi Polisi ini. ii. Menyemak dan menyediakan laporan berkaitan isu keselamatan siber secara berkala. **e. Latihan dan Kesedaran** i. Merancang dan melaksanakan latihan serta program kesedaran keselamatan siber kepada semua pengguna ii. Menyediakan program untuk meningkatkan pemahaman terhadap standard, garis panduan dan prosedur keselamatan ICT. iii. Membudayakan pengetahuan berkaitan teknologi, kawalan maklumat, ancaman siber serta peranan dan tanggungjawab pengguna. **f. Pengurusan Program Keselamatan ICT** Mengurus dan menyelaras keseluruhan program keselamatan ICT di peringkat KPN/Agensi bagi memastikan perlindungan maklumat dan aset ICT dilaksanakan secara	

ID	PENERANGAN	PERANAN
	berkesan dan berterusan.	
5.2.4	**Pengurus ICT** Peranan dan tanggungjawab adalah seperti berikut: a. **Melaksanakan sistem atau aplikasi baharu** Memastikan semua sistem atau aplikasi baharu yang dibangunkan sama ada secara dalaman atau oleh pihak ketiga, terutama yang melibatkan teknologi baharu, mematuhi keperluan keselamatan maklumat seperti yang ditetapkan dalam polisi ini. b. **Peningkatan perisian dan sistem** Meneliti serta meluluskan pembelian atau penaiktarafan perisian dan sistem komputer dengan mengambil kira keperluan keselamatan siber. c. **Perolehan teknologi dan perkhidmatan ICT** Memastikan semua perolehan berkaitan teknologi dan perkhidmatan komunikasi baharu diselaraskan dengan piawaian dan dasar keselamatan maklumat yang berkuat kuasa. d. **Tapisan keselamatan terhadap pembekal dan rakan usaha sama** Menentukan bahawa pihak ketiga yang terlibat menjalani proses tapisan keselamatan yang sewajarnya sebelum diberi akses kepada sistem atau maklumat KPN/Agensi . e. **Pematuhan terhadap dasar dan garis panduan kerajaan** Memastikan pelaksanaan aktiviti ICT	Setiausaha Bahagian / Pengurus ICT / Ketua Cawangan / Ketua Seksyen / Ketua Unit

ID	PENERANGAN	PERANAN
	mematuhi rangka kerja, polisi, pekeliling, garis panduan dan pelan pengurusan keselamatan maklumat kerajaan yang berkaitan dan berkuat kuasa.	
5.2.5	**Pembangun Sistem dan Aplikasi** Pembangun aplikasi berperanan dan bertanggungjawab seperti berikut: a. Membangunkan sistem dan aplikasi seperti yang dipersetujui bersama Pemilik Sistem. b. Menyediakan reka bentuk antaramuka pengguna (UI) dan pengalaman pengguna (UX) yang mesra pengguna dan responsif. c. Membina API atau integrasi antara sistem sedia ada dengan sistem luar (jika perlu). *d.* Berinteraksi dengan pemilik sistem dan pengguna akhir untuk mendapatkan keperluan sistem (*user requirement gathering).* *e.* Menyediakan dokumen mengikut keperluan PPrISA/SOP berkuatkuasa. f. Menyediakan laporan hasil ujian dan dokumentasi teknikal. g. Penyelenggaraan dan Penambahbaikan Sistem h. Melaksanakan penyelenggaraan berkala bagi sistem yang dibangunkan. i. Membuat penambahbaikan *(enhancement)* berdasarkan maklum balas pengguna atau perubahan polisi semasa. j. Menyediakan sistem log perubahan versi dan modul. k. Keselamatan Sistem dan Pematuhan l. Memastikan sistem yang dibangunkan mematuhi keperluan PKS dan PPrISA. m. Melaksanakan mekanisme	Pembangun Sistem dan Aplikasi

ID	PENERANGAN	PERANAN
	pengesahan pengguna *(authentication),* kawalan akses, dan sekuriti pangkalan data. n. Membantu semasa audit keselamatan aplikasi oleh jabatan audit atau pihak ketiga. o. Menyediakan dokumentasi seperti: i. Manual pengguna ii. Manual pentadbir sistem iii. Dokumentasi teknikal (konfigurasi, kod sumber, senibina sistem) iv. Menyediakan changelog setiap kali perubahan dilakukan pada sistem. p. Menyediakan latihan kepada pengguna semasa pelaksanaan sistem *(go-live)* atau semasa penambahbaikan modul. q. Memberi sokongan teknikal kepada pengguna bagi sebarang isu berkaitan sistem. r. Membantu pentadbir sistem dalam menyelesaikan isu teknikal berkaitan perisian. s. Bekerjasama dengan unit pangkalan data, rangkaian, keselamatan ICT dan vendor luaran bagi memastikan kelancaran pembangunan sistem. t. Menyertai Mesyuarat Jawatankuasa Pasukan Kerja, Mesyuarat Jawatankuasa Teknikal, Mesyuarat JPICT dan sesi libat urus berkaitan pembangunan aplikasi jabatan.	
5.2.6	**Pemilik Sistem** Pemilik Sistem terdiri daripada unit atau bahagian yang bertanggungjawab terhadap pembangunan dan pengurusan sesuatu sistem. Pemilik Sistem memainkan peranan penting	Pemilik Sistem

ID	PENERANGAN	PERANAN
	dalam memastikan sistem digunakan secara berkesan dan selamat oleh pengguna yang disasarkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: a. **Promosi dan Penggunaan Sistem** Melaksanakan promosi sistem kepada kumpulan pengguna sasaran bagi menggalakkan penggunaan yang meluas dan berkesan. b. **Pengurusan Akses dan Pengguna** i. Menentukan senarai pengguna serta menetapkan kategori atau tahap capaian pengguna berdasarkan keperluan dan peranan masing-masing. ii. Mengurus senarai pengguna yang terlibat dalam latihan penggunaan sistem. c. **Penguatkuasaan dan Pemantauan** i. Menguatkuasakan penggunaan sistem dalam kalangan pengguna yang berkaitan. ii. Memantau pelaksanaan serta menilai keberkesanan sistem secara berterusan. d. **Peningkatan dan Penambahbaikan** Memaklumkan kepada Pembangun Sistem mengenai sebarang isu, keperluan peningkatan atau penambahbaikan sistem berdasarkan maklum balas dan pemantauan penggunaan. e. **Pelantikan Pentadbir Sistem Aplikasi** Melantik seorang pegawai yang bertanggungjawab sebagai Pentadbir Sistem bagi tujuan penyenggaraan, pemantauan dan penambahbaikan sistem yang dikendalikan.	
5.2.7	**Pentadbir Sistem Aplikasi** Peranan dan tanggungjawab Pentadbir	Pentadbir Sistem Aplikasi

ID	PENERANGAN	PERANAN
	Sistem Aplikasi adalah seperti berikut: **a. Pengurusan Akses Pengguna** i. Mengambil tindakan segera terhadap perubahan status personel seperti berhenti, bertukar Agensi, bercuti panjang, berkursus atau perubahan bidang tugas. ii. Menentukan tahap capaian pengguna adalah tepat dan sah berdasarkan arahan rasmi daripada pemilik maklumat. b. **Pemantauan Aktiviti Sistem Aplikasi** i. Memantau aktiviti capaian ke atas sistem aplikasi secara berkala. ii. Mengenal pasti dan menghentikan serta-merta sebarang aktiviti tidak normal seperti pencerobohan atau pengubahsuaian data tanpa kebenaran. c. **Audit dan Pelaporan** i. Menganalisis dan menyimpan rekod jejak audit *(audit trail)* bagi tujuan pemantauan dan rujukan. ii. Menyediakan laporan berkala mengenai aktiviti capaian sistem kepada pihak berkaitan.	
5.2.8	**Pentadbir Server** Pentadbir Server berperanan dan bertanggungjawab seperti berikut: a. Merancang dan melaksanakan pemasangan server fizikal atau maya *(on-premise* atau *cloud).* b. Mengkonfigurasi sistem operasi server seperti *Windows Server*, Linux (Red	Pentadbir Server

ID	PENERANGAN	PERANAN
	Hat, Ubuntu, CentOS). c. Menyediakan dan menyelenggara Active Directory, DNS, DHCP, File Server, dsb. d. Melaksanakan kawalan keselamatan server: e. Menetapkan polisi kata laluan f. Menyusun peranan pengguna *(role-based access)* g. Mengurus *firewall* server dan antivirus h. Menyemak dan mengemas kini patch keselamatan dan kemas kini sistem secara berkala. i. Menyediakan mekanisme audit dan log capaian ke atas server. j. Memantau status server (CPU, RAM, storage). k. Mengoptimumkan prestasi server untuk mengelakkan downtime atau overload. l. Merancang kapasiti dan membuat perancangan peningkatan sumber *(scalability).* m. Menyelia dan melaksanakan proses sandaran *(backup)* bagi Server secara berkala untuk menjamin pemulihan data sekiranya berlaku kegagalan atau insiden keselamatan n. Menguji kebolehan pemulihan *(restore test)* sekurang-kurangnya 1 kali setahun. o. Menyelia integrasi antara aplikasi dan infrastruktur sedia ada.	
5.2.9	**Pentadbir Pangkalan Data** Pentadbir Pangkalan Data bagi sistem aplikasi adalah berperanan dan bertanggungjawab seperti berikut: a. Menyediakan, memasang dan mengkonfigurasi perisian pangkalan data b. Mewujudkan dan menyelenggara	Pentadbir Pangkalan Data

ID	PENERANGAN	PERANAN
	struktur jadual, skema, indeks, prosedur tersimpan *(stored procedures),* dan fungsi. c. Memastikan pangkalan data beroperasi sepanjang masa dan berada dalam keadaan selamat; d. Mengurus kawalan akses pengguna dan peranan e. Merancang peningkatan kapasiti pangkalan data dan memastikan prestasi pangkalan data di tahap optimum dengan melaksanakan tuning mengikut keperluan; f. Memastikan sandaran *(backup)* dan pemulihan *(restore)* dilaksanakan pada peringkat pangkalan data. g. Memantau capaian ke pangkalan data dan melaporkan kepada ICTSO sekiranya berlaku capaian yang tidak sah; h. Menganalisis log capaian pangkalan data mengikut keperluan dan menyekat aktiviti yang tidak normal; dan i. Menyediakan laporan mengenai capaian pangkalan data mengikut keperluan.	
5.2.10	Pentadbir Rangkaian Peranan dan tanggungjawab adalah seperti berikut: **a. Pentadbiran Akaun dan Akses** Mentadbir akaun pengguna termasuk penciptaan, penyelenggaraan, penggantian dan penyahaktifan akaun berdasarkan keperluan operasi. **b. Polisi Keselamatan dan Kawalan Akses** i. Merangka, melaksana dan menguatkuasakan polisi keselamatan maklumat	Pentadbir Rangkaian

ID	PENERANGAN	PERANAN
	berkaitan perlindungan dan perkongsian data dalam rangkaian. ii. Merancang dan melaksanakan kawalan terhadap ancaman keselamatan serta mengurus penggunaan sumber rangkaian secara berkesan. **c. Pemantauan Rangkaian** i. Memantau aktiviti capaian harian pengguna terhadap rangkaian dan sistem. ii. Menyediakan laporan capaian dan penggunaan rangkaian secara berkala untuk tujuan pemantauan dan penambahbaikan.	
5.2.12	**Pentadbir Pusat Data** Pentadbir Pusat Data adalah berperanan dan bertanggungjawab seperti berikut: a. Memastikan persekitaran fizikal pusat data berada dalam keadaan berfungsi dan selamat; b. Melaksanakan proses sandaran dan pemulihan secara berkala ke atas pangkalan data dan sistem aplikasi; c. Memastikan pusat data sentiasa beroperasi mengikut prosedur yang telah ditetapkan. d. Menyediakan laporan semakan pusat data mengikut keperluan dan	Pentadbir Pusat Data
5.2.13	**Jawatankuasa Pemandu ICT (JPICT)** Peranan dan tanggungjawab Jawatankuasa Pemandu ICT (JPICT) adalah berpandukan Surat Pekeliling Am Bilangan 7 Tahun 2024 (SPA Bil. 7/2024) yang telah dikeluarkan oleh Agensi Digital Negara pada 16 Julai 2024. Pekeliling ini menggantikan Surat Pekeliling Am Bilangan 3 Tahun 2015, dan bertujuan	JPICT

ID	PENERANGAN	PERANAN
	untuk memberikan garis panduan dalam merancang, menyelaras serta menentukan langkah-langkah strategik keselamatan siber di peringkat KPN/Agensi. **Merujuk** Peranan dan tanggungjawab Jawatankuasa Pemandu ICT (JPICT) adalah seperti berikut: a. Menyokong hala tuju strategik pendigitalan dan keselamatan siber organisasi. b. Menilai dan memperakukan cadangan berkaitan projek ICT dan keselamatan maklumat. Memastikan pematuhan terhadap dasar, rangka kerja, dan garis panduan keselamatan digital kerajaan. c. Menyelaras pelaksanaan polisi keselamatan siber merentas semua bahagian dan unit. d. Memantau pelaksanaan dasar, inisiatif serta tindakan pembetulan terhadap isu keselamatan siber	
5.2.14	***Cyber Security Incident Response Team* (CSIRT)** CSIRT bertanggungjawab dalam menangani insiden keselamatan siber secara terancang dan berkesan bagi melindungi aset ICT serta memastikan kesinambungan operasi organisasi. a. Keanggotaan CSIRT adalah seperti berikut: i. **Ketua CSIRT:** Ketua Pegawai Data (CDO) ii. **Pengurus:** Pengurus IT / Pegawai Keselamatan ICT (ICTSO) iii. **Ahli** ● Semua yang dilantik	CSIRT

5.3 Pengasingan Tugas *(Segregation of Duties)*

Pengasingan tugas merujuk kepada amalan memecahkan atau membahagikan tugas dan tanggungjawab yang kritikal kepada beberapa individu atau pasukan berbeza bagi mengelakkan seseorang daripada mempunyai kawalan sepenuhnya ke atas sesuatu sistem, proses atau maklumat.

ID	PENERANGAN	PERANAN
5.3.1	Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. **Pengasingan Tugas** i. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; b. **Perkakasan ICT** Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi; c. **Pengasingan tugas** Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan d. **Semakan dan pemantauan**	Setiausaha Bahagian / Pengurus ICT / Ketua Cawangan / Ketua Seksyen / Ketua Unit

ID	PENERANGAN	PERANAN
	Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	

5.4 Tanggungjawab Pengurusan *(Management Responsibilities)*

Tanggungjawab pengurusan merujuk kepada peranan pihak pengurusan atasan dalam memastikan keselamatan maklumat sentiasa terpelihara. Ini termasuk memastikan dasar dan peraturan dipatuhi, menyediakan sumber yang mencukupi, serta memantau pelaksanaan keselamatan ICT dalam organisasi.

ID	PENERANGAN	PERANAN
5.4.1	Pihak pengurusan hendaklah memastikan semua pengguna mematuhi aspek keselamatan maklumat dan perlindungan aset ICT mengikut dasar, undang-undang dan peraturan yang ditetapkan oleh KPN/Agensi . Pengurusan juga perlu memahami peranan mereka dalam keselamatan maklumat dan mengambil langkah untuk memastikan latihan kesedaran keselamatan ICT dilaksanakan kepada semua pengguna KPN/Agensi . Ini termasuklah pengguna serta pihak ketiga	CDO dan Pengurus ICT

5.5 Hubungan dengan Pihak Berkuasa

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah sentiasa dikekalkan bagi memastikan pengurusan keselamatan maklumat dan insiden dilaksanakan dengan berkesan.

ID	PENERANGAN	PERANAN
5.5.1	Beberapa perkara yang perlu dipatuhi adalah seperti berikut: a. **Pematuhan Perundangan dan Peraturan** KPN/Agensi hendaklah mengenal pasti dan mematuhi semua perundangan, peraturan serta garis panduan yang berkaitan dalam melaksanakan peranan dan tanggungjawab berkaitan keselamatan maklumat dan aset ICT. b. **Prosedur dan Senarai Pihak Berkuasa** KPN/Agensi perlu mewujudkan dan sentiasa mengemas kini prosedur beserta senarai pihak berkuasa perundangan dan pihak yang perlu dihubungi semasa berlaku kecemasan. Pihak berkuasa perundangan termasuk: i. Agensi Peguam Negara ii. Polis Diraja Malaysia (PDRM) iii. Pihak yang perlu dihubungi semasa kecemasan termasuk: ● Pihak utiliti (bekalan air, elektrik) ● Pembekal perkhidmatan ICT dan telekomunikasi ● Perkhidmatan kecemasan (ambulans, bomba, keselamatan dan kesihatan) c. **Laporan Insiden Keselamatan Maklumat**	CSIRT KPN/Agensi

<table>
<tr><th>ID</th><th>PENERANGAN</th><th>PERANAN</th></tr>
<tr><td></td><td>Semua insiden keselamatan maklumat hendaklah dilaporkan dengan segera kepada Agensi Keselamatan Siber Negara (NACSA) selaras dengan Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.

d. Senarai Pihak Berkuasa

Jadual 1: Senarai Pihak Berkuasa
<table>
<tr><th>BIL</th><th>AGENSI</th><th>URUSAN</th></tr>
<tr><td>1</td><td>Agensi Peguam Negara</td><td>Perundangan</td></tr>
<tr><td>2</td><td>Balai POLIS</td><td>Laporan dan Keselamatan</td></tr>
<tr><td>3</td><td>Balai BOMBA</td><td>Laporan dan Keselamatan</td></tr>
<tr><td>4</td><td>Hospital</td><td>Kesihatan</td></tr>
<tr><td>5</td><td>JKR</td><td>Penyelenggaraan</td></tr>
<tr><td>6</td><td>TNB</td><td>Utiliti</td></tr>
</table></td><td></td></tr>
</table>

5.6 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus *(Contact with Special Interest Groups)*

Hubungan yang baik dengan kumpulan berkepentingan khusus, forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan bagi memperkukuh tahap keselamatan maklumat KPN/Agensi .

<table>
<tr><th>ID</th><th>PENERANGAN</th><th>PERANAN</th></tr>
<tr><td>5.6.1</td><td>Penyertaan aktif dalam pertubuhan profesional atau forum keselamatan maklumat adalah digalakkan bagi tujuan berikut:
a. Meningkatkan pengetahuan mengenai amalan terbaik dan perkembangan terkini berkaitan keselamatan maklumat;
b. Memastikan pemahaman yang sentiasa terkini mengenai persekitaran keselamatan maklumat, selaras dengan piawaian seperti ISO/IEC 27002;
c. Menerima amaran awal dan nasihat berkaitan kerentanan serta ancaman keselamatan maklumat semasa;
d. Mendapat akses kepada nasihat pakar dalam bidang keselamatan maklumat;
e. Berkongsi dan bertukar maklumat berkaitan teknologi, produk, ancaman atau kerentanan keselamatan maklumat; dan
f. Menjalin hubungan dengan kumpulan pakar keselamatan maklumat bagi membantu pengurusan insiden keselamatan apabila berlaku.
g. Senarai Pihak Berkepentingan

Jadual 2: Senarai Pihak Berkepentingan
<table><tr><th>BIL</th><th>AGENSI</th><th>URUSAN</th></tr><tr><td>1</td><td>JDN</td><td>Pendigitalan</td></tr><tr><td>2</td><td>NACSA</td><td>Keselamatan ICT</td></tr><tr><td>3</td><td>CGSO</td><td>Keselamatan</td></tr><tr><td>4</td><td>CSIRT</td><td>Laporan Keselamatan</td></tr></table></td><td>CSIRT</td></tr>
</table>

5.7 Perisikan Ancaman *(Threat Intelligence)*

Memberi kesedaran tentang persekitaran ancaman organisasi supaya tindakan mitigasi yang sewajarnya dapat diambil.

ID	PENERANGAN	PERANAN
5.7.1	Maklumat berkaitan ancaman sedia ada atau baharu perlu dikumpul dan dianalisis secara berterusan bagi menyokong usaha melindungi sistem dan maklumat KPN/Agensi . Tindakan ini bertujuan untuk: a. Memudahkan pelaksanaan tindakan pencegahan dan pemulihan serta mengelakkan ancaman daripada mendatangkan kemudaratan kepada organisasi;dan b. Mengurangkan impak terhadap keselamatan maklumat sekiranya ancaman berlaku. c. Risikan ancaman haruslah: i. **Relevan** Maklumat yang diperoleh mestilah mempunyai kaitan terus dengan ancaman yang boleh menjejaskan operasi atau keselamatan maklumat organisasi; ii. **Berwawasan** Risikan perlu memberi gambaran yang jelas, menyeluruh dan mendalam mengenai bentuk dan corak ancaman, agar organisasi dapat membuat persediaan awal dan mengurus risiko dengan lebih berkesan; iii. **Kontekstual**	ICTSO dan CSIRT

ID	PENERANGAN	PERANAN
	Maklumat tambahan seperti masa, lokasi kejadian, cara kejadian berlaku, dan kaitannya dengan insiden terdahulu atau kejadian serupa di agensi lain dapat membantu organisasi memahami situasi dengan lebih jelas dan tepat; dan iv. **Boleh Diambil Tindakan** Maklumat risikan yang diterima perlu cukup jelas, tepat dan boleh digunakan untuk membolehkan organisasi bertindak segera dalam mencegah atau mengurangkan kesan daripada ancaman.	

5.8 Keselamatan Maklumat dalam Pengurusan Projek *(Information Security in Project Management)*

Keselamatan maklumat hendaklah diberi perhatian dalam pengurusan projek tanpa mengira kerumitan, saiz, tempoh, disiplin atau skop pelaksanaannya.

ID	PENERANGAN	PERANAN
5.8.1	Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. keselamatan maklumat perlu di integrasikan bagi setiap pengurusan projek; b. objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;	Pegawai Keselamatan /CSIRT

ID	PENERANGAN	PERANAN
	d. kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber; e. penyediaan spesifikasi perolehan hendaklah memasukkan keperluan pasukan projek pihak pembekal yang mempunyai pensijilan keselamatan maklumat; f. Pertimbangan dan aktiviti keselamatan maklumat hendaklah dilaksanakan pada peringkat yang ditetapkan, selaras dengan tadbir urus projek sedia ada seperti Jawatankuasa Teknikal Projek atau Jawatankuasa Pemandu Projek; dan g. Peranan dan tanggungjawab berkaitan keselamatan maklumat dalam sesuatu projek hendaklah ditakrif dan ditentukan dengan jelas sejak awal pelaksanaan.	

5.9 Inventori Maklumat Dan Aset Lain Yang Berkaitan *(Inventory of Information And Other Associated Assets)*

ID	PENERANGAN	PERANAN
5.9.1	KPN/Agensi bertanggungjawab untuk menyokong dan melindungi semua aset ICT dengan sewajarnya. Tanggungjawab ini merangkumi perkara-perkara berikut: a. Pelantikan Pegawai Penerima Aset KPN/Agensi hendaklah mengenal pasti dan melantik Pegawai Penerima Aset bagi setiap bahagian untuk menguruskan penerimaan aset ICT yang diperoleh melalui projek-projek ICT. b. Pengurusan Aset ICT Semua aset ICT hendaklah dikenal pasti, diklasifikasi, didokumenkan,	Pegawai Aset, Pegawai Penerima Aset dan warga

ID	PENERANGAN	PERANAN
	diselenggara dan dilupuskan mengikut keperluan semasa. Rekod maklumat aset perlu dikemas kini selaras dengan arahan dan peraturan yang berkuatkuasa. c. Pemilikan dan Kawalan Akses Setiap aset ICT perlu mempunyai pemilik yang sah dan hanya boleh dikendalikan oleh pengguna yang diberi kebenaran. d. Penyelenggaraan Inventori Inventori maklumat dan aset berkaitan hendaklah sentiasa tepat, terkini dan konsisten. e. Pengesahan Penempatan Aset Pegawai Aset hendaklah membuat pengesahan ke atas penempatan fizikal aset ICT bagi memastikan kawalan dan pemantauan aset dilaksanakan dengan berkesan.	
5.9.2	**Pemilikan Aset *(Ownership Of Assets)*** Setiap aset yang diselenggara hendaklah merupakan hak milik KPN/Agensi . Pemilik aset bertanggungjawab untuk memastikan pengurusan aset dilaksanakan dengan teratur dan berlandaskan peraturan yang ditetapkan. Tanggungjawab tersebut merangkumi perkara berikut: a. **Pendaftaran Aset** Memastikan setiap aset didaftarkan dalam senarai aset mengikut klasifikasi yang ditetapkan dan diserahkan kepada pemilik aset yang sah. b. **Penyelenggaraan Aset** Memastikan semua jenis aset dipelihara, diselenggara dan sentiasa dalam keadaan baik. c. **Semakan Akses** Mengenal pasti dan menyemak semula akses ke atas aset penting	Pegawai Aset dan Warga

ID	PENERANGAN	PERANAN
	secara berkala, berdasarkan polisi kawalan capaian yang berkuat kuasa. **d. Pengendalian Aset Semasa Pelupusan** Memastikan proses pengendalian aset dilaksanakan dengan teratur dan selamat apabila aset dihapus atau dilupuskan.	
5.9.3	**Pengelasan Maklumat Aset *(Information Classification Assets)*** Memastikan setiap aset ICT dikenal pasti dan diklasifikasikan mengikut kategori klasifikasi yang ditetapkan bagi membolehkan kawalan keselamatan maklumat dilaksanakan secara berkesan.	Pegawai Pengkelas/ Aset

5.10 Penggunaan Maklumat Yang Boleh Diterima Dan Aset Lain Yang Berkaitan *(Acceptable Use Of Information And Other Associated Assets)*

ID	PENERANGAN	PERANAN
5.10.1	**Pengendalian Aset *(Handling Of Assets)*** Memastikan semua pengguna menggunakan aset ICT hanya untuk urusan rasmi selaras dengan tugas dan tanggungjawab yang ditetapkan. Segala aktiviti pengendalian aset dan maklumat seperti pengumpulan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, pertukaran dan pemusnahan hendaklah dilaksanakan dengan mematuhi langkah-langkah keselamatan berikut: a. Mengelakkan pendedahan maklumat kepada pihak yang tidak dibenarkan. b. Memastikan maklumat adalah tepat, lengkap dan dikemas kini secara berkala. c. Menyediakan maklumat dalam keadaan sedia untuk digunakan apabila diperlukan. d. Menjaga kerahsiaan kata laluan dan	Pegawai Aset dan Pengguna

ID	PENERANGAN	PERANAN
	maklumat akses lain. e. Mematuhi semua standard, prosedur, langkah dan garis panduan keselamatan maklumat yang berkuat kuasa. f. Memberikan perhatian khusus terhadap maklumat terperingkat semasa proses penciptaan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, pertukaran dan pelupusan. g. Menjamin kerahsiaan berkaitan langkah keselamatan siber agar tidak didedahkan kepada umum. h. Melaksanakan kawalan akses mengikut keperluan perlindungan berdasarkan tahap pengelasan maklumat. i. Menyimpan dan menyelenggara rekod pengguna yang dibenarkan bagi capaian kepada maklumat dan aset berkaitan.	

5.11 Pemulangan aset *(Return of Assets)*

ID	PENERANGAN	PERANAN
5.11.1	Aset yang dipinjam atau disewa hendaklah dipulangkan dan disanitasi mengikut tatacara yang ditetapkan dalam Surat Pekeliling Am Bilangan 4 Tahun 2022 – Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam.	Pegawai Aset dan Pengguna

5.12 Pengelasan Maklumat *(Classification of Information)*

ID	PENERANGAN	PERANAN
5.12.1	Maklumat hendaklah diklasifikasikan oleh Pegawai Pengelas yang dilantik berdasarkan keperluan keselamatan maklumat seperti yang dinyatakan dalam Arahan Keselamatan. (Semakan dan Pindaan 2017).	Pegawai pengkelas/ Pegawai Rekod Agensi /Pegawai

ID	PENERANGAN	PERANAN
	Pengelasan ini perlu mengambil kira tiga aspek utama keselamatan maklumat, iaitu **kerahsiaan, integriti** dan **ketersediaan**, serta keperluan pihak-pihak yang berkepentingan. Klasifikasi dan kawalan perlindungan maklumat perlu: a. Menyokong keperluan perkhidmatan untuk berkongsi atau menyekat akses kepada maklumat; b. Melindungi maklumat daripada akses yang tidak dibenarkan, kehilangan, atau pengubahan tanpa kebenaran; c. Mengikut keperluan undang-undang dan garis panduan sedia ada. Selain maklumat, aset ICT lain juga boleh diklasifikasikan berdasarkan jenis maklumat yang disimpan, diproses atau dikendalikan oleh aset tersebut.Pengelasan maklumat mestilah berpandukan kepada: a. Akta Rahsia Rasmi 1972; b. Akta Arkib Negara 2003 (Akta 629); c. Surat Pekeliling Am Bilangan 5 Tahun 2007 – Pengurusan Rekod Awam; d. Piawaian, tatacara dan garis panduan keselamatan yang dikeluarkan oleh pihak berkuasa berkaitan. e. Maklumat yang telah diklasifikasikan perlu dilabel dengan betul dan disimpan mengikut tahap keselamatan.	Pengawal Dokumen

5.13 Pelabelan Maklumat *(Labelling of Information)*

ID	PENERANGAN	PERANAN
5.13.1	Setiap maklumat yang diklasifikasikan hendaklah dilabel dengan jelas dan tepat mengikut Arahan Keselamatan semasa. Pelabelan bertujuan untuk: a. Memastikan setiap maklumat menerima tahap perlindungan yang	Pegawai pengkelas/ Pegawai Rekod Agensi /Pegawai Pengawal Dokumen

ID	PENERANGAN	PERANAN
	sesuai berdasarkan klasifikasinya; b. Mengenal pasti tahap keselamatan maklumat dengan cepat oleh semua pengguna yang berkenaan; dan c. Membantu dalam pengendalian, penyimpanan dan pelupusan maklumat secara betul dan selamat. d. Maklumat yang diklasifikasikan hendaklah dilabelkan oleh Pegawai Pengelas atau individu yang diberi kuasa mengikut garis panduan yang ditetapkan oleh Arkib Negara Malaysia dan peraturan keselamatan siber semasa. Contoh Kaedah Pelabelan Maklumat: i. **Label fizikal** – Pelekat atau cetakan jelas pada dokumen fizikal (contoh: **"SULIT", "RAHSIA"**). ii. ***Header* dan *footer*** – Tanda pada bahagian atas dan bawah dokumen digital untuk menunjukkan peringkat keselamatan. iii. **Cop getah *(rubber stamp)*** – Digunakan pada dokumen cetakan untuk menunjukkan klasifikasi maklumat dengan cepat. e. Semua pelabelan mestilah konsisten dan mengikut format rasmi yang telah ditetapkan untuk mengelakkan kekeliruan dan menjamin keselamatan maklumat organisasi.	

5.14 Pemindahan Data Dan Maklumat *(Information transfer)*

ID	PENERANGAN	PERANAN
5.14.1	Pemindahan atau pertukaran data, maklumat dan perisian antara KPN/Agensi dan pihak luar hendaklah dilakukan dengan cara yang	CDO / ICTSO / Pentadbir Sistem /

ID	PENERANGAN	PERANAN
	selamat dan terkawal, bagi mengelakkan pendedahan, kehilangan atau pengubahsuaian maklumat yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: a. **Polisi dan Prosedur Pemindahan** Semua pemindahan maklumat perlu mengikuti polisi, prosedur dan kawalan yang formal, bagi memastikan maklumat dipindahkan dengan selamat melalui apa jua saluran komunikasi, termasuk rangkaian internet, storan fizikal, atau peranti mudah alih. b. **Perjanjian dengan Pihak Luar** Terma pemindahan maklumat dan perisian antara KPN/Agensi dan pihak luar perlu dinyatakan dengan jelas dalam perjanjian (jika perlu), bagi melindungi hak dan tanggungjawab semua pihak. **c. Perlindungan Media** Media storan yang digunakan untuk menyimpan atau memindahkan maklumat (contohnya: pemacu USB, cakera keras, cakera optik) hendaklah dilindungi daripada akses tidak sah, kehilangan atau kerosakan fizikal. **d. Keselamatan E-mel** Maklumat yang dihantar melalui e-mel rasmi perlu dilindungi dengan dilindungi sebaik-baiknya.	Pengguna dan pembekal
5.14.2	**Perjanjian Mengenai Pemindahan Data Dan Maklumat *(Agreements On Information Transfer)*** KPN/Agensi perlu memastikan aspek keselamatan maklumat diberi perhatian apabila berlaku pemindahan data dan maklumat organisasi kepada pihak luar. Sebarang pemindahan hendaklah disokong dengan perjanjian bertulis yang jelas, bagi melindungi kepentingan organisasi. Perkara	CDO dan Ketua Agensi / Ketua Bahagian

ID	PENERANGAN	PERANAN
	yang perlu dipertimbangkan adalah seperti berikut: a. **Kawalan Penghantaran dan Penerimaan** Pengurus ICT bertanggungjawab mengawal setiap pemindahan data dan maklumat, termasuk penghantaran dan penerimaan, bagi menjamin keselamatan serta integriti maklumat. **b. Pengesanan dan Pengesahan Pemindahan** Prosedur perlu disediakan bagi memastikan setiap pemindahan maklumat boleh dikesan, direkod dan tidak boleh dinafikan oleh mana-mana pihak yang terlibat. **c. Tanggungjawab Terhadap Risiko** KPN/Agensi perlu mengenal pasti pihak yang bertanggungjawab sekiranya berlaku insiden keselamatan maklumat semasa atau selepas pemindahan data dilakukan. **d. Perlindungan Sepanjang Kitaran Data** KPN/Agensi hendaklah memastikan perlindungan data meliputi semua peringkat iaitu: i. Semasa digunakan *(data in use)* *ii.* Semasa dalam pergerakan *(data in transit)* iii. Semasa disimpan *(data at rest)* iv. serta mengambil langkah bagi menghalang ketirisan data. e. **Pematuhan Polisi dan Dasar Berkaitan** Semua pemindahan data perlu merujuk dan mematuhi Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional semasa.	

ID	PENERANGAN	PERANAN
5.14.3	**Pesanan Elektronik *(Electronic Messaging)*** Maklumat yang dihantar atau diterima melalui pesanan elektronik seperti e-mel perlu dilindungi dan dikendalikan dengan mematuhi peraturan serta arahan rasmi yang berkuat kuasa. Tujuannya adalah untuk memastikan keselamatan, kerahsiaan, integriti dan ketersediaan maklumat sentiasa terpelihara. Perkara yang perlu dipatuhi adalah seperti berikut: a. **Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi - Agensi Kerajaan (Bilangan 1 Tahun 2003)** Menetapkan kaedah penggunaan yang betul, selamat dan beretika bagi mel elektronik dan internet. b. **Arahan Setiausaha Majlis Keselamatan Negara (MKN) (Bilangan 1 Tahun 2013)** Mengenai pematuhan terhadap tatacara penggunaan e-mel dan internet bagi menjamin keselamatan komunikasi elektronik kerajaan. c. **Surat Arahan Ketua Agensi (Bertarikh 1 Jun 2007)** Mengenai langkah-langkah keselamatan tambahan dalam penggunaan e-mel rasmi di Agensi kerajaan. d. **Garis Panduan Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (MyGovUC)** Bagi memastikan penggunaan e-mel rasmi melalui perkhidmatan MyGovUC adalah teratur, selamat dan mematuhi polisi yang ditetapkan. e. **Perekodan Emel Rasmi** Semua e-mel rasmi hendaklah direkodkan ke dalam sistem Document Management System 2.0 (DDMS 2.0)	Warga

ID	PENERANGAN	PERANAN
	sebagai rekod rasmi kerajaan.	
5.14.4	Keselamatan dalam pemindahan atau pertukaran data, maklumat dan perisian antara KPN/Agensi dengan pihak luar hendaklah dipastikan agar maklumat sentiasa dilindungi dan tidak mudah terdedah. Perkara yang perlu dipatuhi adalah seperti berikut: a. Pemindahan data dan maklumat hendaklah mematuhi polisi, prosedur dan kawalan yang sedang berkuat kuasa bagi melindungi keselamatan komunikasi. b. Terma pemindahan data, maklumat dan perisian antara KPN/Agensi dan pihak luar hendaklah dinyatakan dalam perjanjian bertulis sekiranya perlu. c. Media yang mengandungi maklumat perlu dilindungi daripada sebarang akses yang tidak dibenarkan. d. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	CDO / ICTSO / Pentadbir Sistem / Pengguna dan pembekal

5.15 Kawalan capaian *(Access Control)*

ID	PENERANGAN	PERANAN
5.15.1	Capaian kepada maklumat dan aset berkaitan perlu diberikan, disemak semula, diubah atau ditamatkan berdasarkan tahap keperluan dan klasifikasi keselamatan maklumat. Tindakan ini bertujuan untuk memastikan pematuhan terhadap keperluan keselamatan dalam mengawal akses ke atas aset ICT. Perkara yang perlu dipertimbangkan dalam pelaksanaan kawalan capaian termasuk: a. Menentukan jenis capaian yang diperlukan bagi individu atau kumpulan	ICTSO, Pentadbir Sistem Aplikasi

ID	PENERANGAN	PERANAN
	terhadap maklumat dan aset berkaitan; b. Menyediakan kawalan keselamatan untuk aplikasi yang digunakan; c. Melaksanakan kawalan capaian fizikal yang bersesuaian; d. Penetapan kebenaran dan perkongsian maklumat berdasarkan tahap keselamatan dan klasifikasi maklumat; *e.* Pengawalan capaian istimewa *(privileged access);* f. Pengasingan tugas dan tanggungjawab berdasarkan keperluan dan tahap capaian; g. Permohonan akses secara rasmi; h. Mengurus dan menyemak hak akses pengguna secara berkala; dan i. Merekod dan menyemak jejak audit *(Audit trail)* bagi mengesan aktiviti capaian yang mencurigakan.	
5.15.2	**Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian *(Access To Networks And Network Services)*** Pengurusan capaian ke atas rangkaian bertujuan untuk menghalang akses yang tidak sah atau tanpa kebenaran ke atas perkhidmatan rangkaian, sama ada rangkaian berwayar atau tanpa wayar. Penggunaan perkhidmatan rangkaian hendaklah diberikan kepada pengguna berdasarkan tugas dan skop kerja masing-masing. Semua sistem, aplikasi dan pengguna perlu mematuhi kawalan capaian yang ditetapkan seperti berikut: a. Hak akses yang dibenarkan adalah selari dengan klasifikasi maklumat yang ditetapkan; b. Hak akses fizikal yang dibenarkan adalah selari dengan keperluan keselamatan;	ICTSO, Pengurus ICT dan Pentadbir Rangkaian

ID	PENERANGAN	PERANAN
	c. Mengenalpasti entiti mengikut kelayakan hak akses yang dibenarkan seperti pelawat hanya dibenarkan mengakses rangkaian tanpa wayar *(WiFi Guest);* dan d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
5.15.3	Kawalan capaian bertujuan untuk mengurus, mengawasi dan melindungi akses terhadap maklumat dan aset KPN/Agensi dengan selamat. Ia merangkumi aspek operasi dan pengurusan bagi memastikan KPN/Agensi mencapai objektif, sasaran dan hasil yang ditetapkan. Fungsi kawalan capaian hendaklah dilaksanakan dengan mengambil kira perkara-perkara berikut: a. **Pematuhan Undang-Undang dan Polisi** Mematuhi undang-undang, peraturan serta polisi yang berkaitan dengan keselamatan maklumat yang sedang berkuat kuasa. b. **Pelaksanaan Dasar dan Prosedur Keselamatan** Memastikan dasar, prosedur dan amalan keselamatan maklumat dilaksanakan dengan betul dan konsisten oleh semua pihak yang terlibat. **c. Pengurusan Risiko** Mengenal pasti, menilai dan mengurus risiko keselamatan maklumat berkaitan capaian terhadap maklumat dan aset organisasi. d. **Perlindungan Maklumat dan Data** Menjamin keselamatan maklumat	Pegawai Keselamatan, BPM

ID	PENERANGAN	PERANAN
	serta data organisasi dengan mengaplikasikan kawalan keselamatan yang sesuai mengikut klasifikasi maklumat. e. **Kesedaran dan Latihan** Meningkatkan kesedaran dan kefahaman dalam kalangan warga kerja terhadap kepentingan kawalan capaian dan amalan keselamatan maklumat. f. **Pemantauan Prestasi Keselamatan** Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenalpasti peningkatan dan kesan tindakan yang diperlukan.	

5.16 Pengurusan Identiti *(Identity Management)*

ID	PENERANGAN	PERANAN
5.16.1	**Pendaftaran Dan Pembatalan Pengguna *(User Registration And De-Registration)*** Setiap pengguna bertanggungjawab terhadap penggunaan aset ICT yang diperuntukkan kepada mereka. Bagi memastikan pengenalpastian pengguna dan aktiviti yang dijalankan direkod secara sah dan selamat, garis panduan berikut hendaklah dipatuhi: a. **Penggunaan Akaun Sah** Hanya akaun yang diperuntukkan oleh KPN/Agensi dibenarkan untuk digunakan bagi mengakses sistem atau perkhidmatan ICT. b. **Akaun Pengguna Unik dan Bertanggungjawab** Akaun pengguna mestilah unik, dan setiap pengguna bertanggungjawab sepenuhnya terhadap akaun yang	Pengguna dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	diberikan selepas pengesahan penerimaan dibuat. c. **Kelulusan Perubahan Akses** Sebarang pindaan terhadap tahap akses mestilah mendapat kelulusan rasmi daripada Pemilik Sistem terlebih dahulu. d. **Penggantungan atau Penarikan Balik Akaun** Akaun boleh digantung atau ditarik balik sekiranya pengguna didapati melanggar peraturan keselamatan atau polisi ICT yang ditetapkan. e. **Larangan Perkongsian Akaun** Penggunaan atau perkongsian akaun milik orang lain adalah dilarang sama sekali. f. **Penamatan Akaun** Akaun pengguna perlu ditamatkan apabila berlaku perubahan status seperti berikut: i. Pertukaran bidang tugas; ii. Pertukaran ke KPN atau Agensilain; iii. Persaraan; atau iv. Penamatan perkhidmatan. g. **Semakan Akses Berkala** Proses semakan capaian pengguna perlu dilaksanakan secara berkala bagi memastikan ketepatan, keperluan dan kelulusan terhadap akses yang diberikan. h. **Larangan Penyamaran** Pengguna dilarang menggunakan identiti orang lain atau menyamar dalam mana-mana perkhidmatan	

ID	PENERANGAN	PERANAN
	dalam talian.	
5.16.2	**Pengurusan Identiti *(Identity Management)*** Pengurusan identiti melibatkan pengendalian profil warga bermula daripada penciptaan rekod pengguna baharu sehingga penamatan profil apabila warga meninggalkan perkhidmatan seperti persaraan, peletakan jawatan, atau kematian. Ia juga merangkumi kawalan capaian pengguna terhadap aset ICT milik KPN/Agensi. Semua proses berkaitan pendaftaran, pengemaskinian dan penamatan akaun pengguna hendaklah dilaksanakan mengikut prosedur yang telah ditetapkan. Tujuannya adalah untuk memastikan bahawa hanya individu yang sah dan diberi kuasa sahaja boleh mengakses sistem dan maklumat organisasi. Proses pengurusan identiti perlu merangkumi perkara berikut: a. **Pengenalpastian Keperluan Tugasan** Identiti pengguna diwujudkan berdasarkan keperluan tugas atau peranan yang berkaitan dalam organisasi. b. **Pengesahan Identiti** Identiti pengguna yang memohon akaun hendaklah disahkan terlebih dahulu sebelum akaun diwujudkan. **c. Pengwujudan Akaun** Akaun pengguna hendaklah diwujudkan mengikut proses yang ditetapkan. **d. Konfigurasi dan Pengaktifan Akaun** Akaun yang diwujudkan perlu	Ketua Agensi/ Penyelia/ Pemilik Sistem

ID	PENERANGAN	PERANAN
	dikonfigurasi dan diaktifkan sebelum digunakan. e. **Penyediaan atau Pembatalan Hak Akses** Menyediakan atau membatalkan hak akses berdasarkan kelulusan atau pemaklum; dan f. **Penamatan Akaun** Akaun pengguna perlu dipadamkan atau dinyahaktif dengan segera apabila tidak lagi diperlukan, sama ada kerana pertukaran tugas, penamatan perkhidmatan atau sebab-sebab lain yang sah.	

5.17 Maklumat Pengesahan *(Authentication Information)*

ID	PENERANGAN	PERANAN
5.17.1	**Pengurusan Maklumat Pengesahan Rahsia *(Management of Secret Authentication Information)*** Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Perkara-perkara penting dalam pengurusan maklumat pengesahan rahsia termasuk: a. **Penjanaan Kata Laluan Sementara yang Unik** Setiap pengguna baharu hendaklah diberikan kata laluan sementara yang unik semasa pendaftaran, dan diwajibkan menukarnya semasa log masuk kali pertama. b. **Prosedur Pengesahan Akaun** Mewujudkan dan melaksanakan	ICTSO dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	prosedur pengesahan identiti bagi setiap permohonan baharu, penggantian akaun, atau maklumat pengesahan sementara. c. **Penghantaran Maklumat Secara Selamat** Semua maklumat kata laluan atau pengesahan hendaklah dihantar kepada pengguna melalui kaedah yang selamat dan disulitkan *(encrypted).* d. **Penukaran Kata Laluan Lalai** Kata laluan lalai yang diberikan hendaklah ditukar serta-merta selepas pemasangan sistem, perisian atau perkakasan. e. **Penyimpanan Maklumat Rahsia yang Selamat** Semua maklumat pengesahan rahsia mesti disimpan menggunakan kaedah yang diluluskan dan selamat bagi mengelakkan capaian tanpa kebenaran.	
5.17.2	**Penggunaan Maklumat Pengesahan Rahsia *(Use Of Secret Authentication Information)*** Setiap pengguna bertanggungjawab untuk menggunakan maklumat pengesahan rahsia seperti kata laluan dan kod keselamatan dengan selamat serta mematuhi dasar keselamatan siber. Tanggungjawab Pengguna seperti yang berikut: **a. Memahami Polisi dan Tanggungjawab**	Pengguna, Pentadbir Sistem dan Pengurus ICT

ID	PENERANGAN	PERANAN
	i. Membaca, memahami dan mematuhi Polisi Keselamatan Siber KPN/Agensi ii. Menyedari implikasi keselamatan siber akibat daripada tindakan sendiri. iii. Menjaga kerahsiaan dan keselamatan maklumat organisasi. b. **Langkah Perlindungan Maklumat:** i. Mengelakkan pendedahan maklumat kepada pihak tidak dibenarkan. ii. Memastikan maklumat adalah tepat, lengkap dan sedia digunakan. iii. Menjaga kerahsiaan kata laluan dengan tidak berkongsi atau menulisnya di tempat tidak selamat. iv. Mematuhi semua piawaian, prosedur dan garis panduan keselamatan yang ditetapkan. v. Memberi perhatian khusus terhadap pengurusan maklumat terperingkat dalam semua fasa (cipta, simpan, hantar, ubah dan musnah). vi. Melindungi langkah keselamatan siber daripada didedahkan kepada umum. c. **Tindakan Sekiranya Berlaku Kompromi:** i. Menukar maklumat pengesahan rahsia dengan segera sekiranya terdapat tanda atau makluman kompromi.	

ID	PENERANGAN	PERANAN
	ii. Melaporkan sebarang aktiviti yang mencurigakan atau mengancam keselamatan kepada Pegawai ICTSO dengan segera. d. **Amalan Pengurusan Kata Laluan yang Selamat:** i. Memilih kata laluan yang kukuh dan sukar diteka. ii. Tidak menggunakan semula kata laluan yang mudah dijangka. iii. Tidak berkongsi kata laluan dengan sesiapa.	
5.17.3	**Sistem Pengurusan Kata Laluan *(Password Management System)*** Pengurusan kata laluan mestilah mematuhi amalan terbaik dan prosedur yang ditetapkan. Garis panduan berikut perlu dipatuhi: a. Kata laluan hendaklah sentiasa dilindungi dan tidak boleh dikongsi dalam apa jua keadaan. b. Pengguna mesti menukar kata laluan dengan segera sekiranya terdapat syak berlaku kebocoran atau kompromi terhadap kata laluan. c. Panjang kata laluan hendaklah sekurang-kurangnya **DUA BELAS (12) AKSARA,** merangkumi gabungan huruf, nombor dan aksara khas. **PENGECUALIAN** hanya dibenarkan bagi perkakasan atau perisian yang mempunyai had keupayaan pengurusan kata laluan. d. Kata laluan mestilah diingati sendiri oleh pengguna dan **TIDAK BOLEH**	Pengguna, Pentadbir Sistem, ICTSO, Pengurus ICT

ID	PENERANGAN	PERANAN
	dicatat, disimpan atau didedahkan dalam apa-apa bentuk sekali pun. e. Kata laluan untuk fungsi paparan kunci *(lock screen)* perlu diaktifkan, terutamanya pada komputer yang digunakan di ruang bersama. f. Pengguna diwajibkan untuk **MENUKAR** kata laluan sekurang-kurangnya **SEKALI** dalam tempoh satu (1) tahun. g. Kata laluan tidak boleh menyerupai ID atau nama pengguna. h. Percubaan untuk memasukkan kata laluan hanya dibenarkan maksimum **TIGA (3)** kali sahaja. Selepas itu, akses ke sistem akan disekat sehingga ID capaian diaktifkan semula oleh pentadbir. i. Setiap sistem yang dibangunkan hendaklah mempunyai fungsi untuk membolehkan pengguna menukar kata laluan mereka sendiri.	

5.18 Hak Capaian *(Access Rights)*

ID	PENERANGAN	PERANAN
5.18.1	**Pendaftaran Dan Pembatalan Hak Akses** Proses pendaftaran dan pembatalan hak akses, sama ada secara fizikal atau logikal, hendaklah dilaksanakan berdasarkan prosedur yang ditetapkan. Langkah-langkah berikut perlu dipatuhi: a. Mendapatkan kelulusan daripada pemilik maklumat dan aset yang berkaitan sebelum memberikan hak	Pentadbir Sistem dan Pengurus ICT

ID	PENERANGAN	PERANAN
	akses. b. Mengambil kira dasar, polisi atau peraturan khas yang berkaitan dengan pengurusan hak akses. c. Memastikan pengasingan peranan *(role segregation)* dalam pemberian hak akses. d. Menamatkan hak akses dengan segera sekiranya pengguna tidak lagi memerlukan akses kepada maklumat atau sistem. e. Memberikan hak akses sementara kepada warga kontrak atau individu yang hanya memerlukan akses untuk tempoh tertentu sahaja. f. Mengesahkan tahap akses yang diberikan adalah mengikut had capaian dan selari dengan keperluan keselamatan maklumat. g. Hak akses hanya boleh diaktifkan selepas prosedur pengesahan diluluskan. h. Menyelenggara rekod hak akses secara berpusat untuk tujuan pemantauan dan audit. i. Melaksanakan perubahan hak akses bagi pengguna yang bertukar peranan, jawatan atau bertukar ke organisasi lain. j. Menamatkan atau mengemas kini hak akses fizikal dan logikal mengikut keperluan semasa dan status pengguna.	

ID	PENERANGAN	PERANAN
	k. Menyelenggara rekod perubahan hak akses bagi tujuan rekod dan rujukan.	
5.18.2	**Kajian Semula Hak Akses Pengguna *(Review Of User Access Rights)*** Kajian semula terhadap hak akses pengguna hendaklah dilaksanakan secara berkala bagi memastikan kawalan akses kekal relevan, terkawal dan selamat. Semakan ini perlu merangkumi perkara-perkara berikut: a. Perubahan dalam organisasi, seperti pertukaran pusingan kerja, kenaikan pangkat, penurunan pangkat, atau penamatan perkhidmatan. b. Semakan ke atas hak akses istimewa *(privileged access)* bagi memastikan ia masih diperlukan dan digunakan secara wajar. c. Pelaksanaan semakan hak akses secara berkala, atau berdasarkan keperluan semasa.	ICTSO dan Pentadbir Sistem
5.18.3	**Pembatalan Atau Pelarasan Hak Akses *(Removal Or Adjustment Of Access Rights)*** Hak akses pengguna kepada maklumat dan aset yang berkaitan hendaklah disemak dan diselaraskan atau ditamatkan sebelum sebarang perubahan atau penamatan pekerjaan berdasarkan penilaian faktor risiko seperti: a. Pengguna atau pengurusan mengemukakan sebarang permohonan penamatan dan perubahan. b. Tanggungjawab semasa pengguna dalam organisasi.	Pentadbir Sistem dan Pengurus ICT

ID	PENERANGAN	PERANAN
	c. Hak akses bagi pengguna luar ke atas kemudahan pemprosesan data atau maklumat hendaklah ditamatkan selepas berlakunya penamatan perkhidmatan, kontrak atau perjanjian, atau diselaraskan sekiranya terdapat perubahan dalam struktur atau peranan organisasi.	

5.19 Keselamatan Maklumat Dalam Hubungan Pembekal *(Information Security Policy for Supplier Relationships)*

ID	PENERANGAN	PERANAN
5.19.1	Bagi mengurangkan risiko terhadap aset KPN/Agensi, keperluan keselamatan maklumat hendaklah **DITAKRIFKAN, DIPERSETUJUI, DILAKSANAKAN** dan **DIDOKUMENTASIKAN** bersama pembekal. Perkara-perkara berikut perlu dipertimbangkan: a. Pengurusan Akses dan Maklumat oleh Pembekal i. Pengelasan maklumat berdasarkan kategori rekod rasmi Kerajaan. ii. Kawalan dan pemantauan akses pembekal kepada sistem atau maklumat. iii. Menetapkan keperluan minimum keselamatan maklumat dalam setiap perjanjian dengan pembekal. iv. Penetapan jenis-jenis obligasi keselamatan maklumat yang perlu dipatuhi oleh pembekal.	Pegawai Keselamatan/ CSIRT

ID	PENERANGAN	PERANAN
	v. Pelan kontingensi bagi memastikan kesinambungan dan ketersediaan kemudahan pemprosesan maklumat. vi. Pelaksanaan program kesedaran keselamatan siber kepada pembekal yang melibatkan sistem atau maklumat organisasi. vii. Pembekal hendaklah mematuhi semua arahan keselamatan yang sedang berkuat kuasa. **b. Keperluan Keselamatan Pihak Ketiga** Pembekal, termasuk warga pihak ketiga, hendaklah mematuhi perkara berikut: i. Polisi Keselamatan Siber (PKS) Kementerian Perpaduan Negara dan Agensi. ii. Akta Rahsia Rasmi 1972 (ARA 1972). iii. Tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO). **c. Pengurusan Risiko Penggunaan Perkhidmatan Pembekal** i. Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk atau perkhidmatan pembekal. ii. Termasuk juga prosedur penamatan penggunaan produk/perkhidmatan pembekal secara selamat dan terkawal. **d. Penamatan Hubungan dengan**	

ID	PENERANGAN	PERANAN
	Pembekal Semasa penamatan hubungan dengan pembekal, langkah-langkah keselamatan berikut hendaklah diambil untuk melindungi maklumat dan aset: i. Pengendalian maklumat; ii. Menentukan pemilikan harta intelek; iii. Pemindahan maklumat sekiranya berlaku pertukaran pihak ketiga; iv. Pengurusan rekod; v. Pemulangan aset; vi. Pelupusan selamat maklumat dan aset lain yang berkaitan;dan vii. Keperluan kerahsiaan berterusan	

5.20 Menangani Keselamatan Dalam Perjanjian *(Addressing Security Within Supplier Agreements)*

ID	PENERANGAN	PERANAN
5.20.1	Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui bersama setiap pembekal yang terlibat dalam mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT berkaitan maklumat organisasi.	Pengguna
5.20.2	Pembekal bertanggungjawab untuk memastikan semua warga mereka mematuhi kawalan keselamatan maklumat dan melaksanakan tindakan kawalan yang diperlukan pada setiap masa, selaras dengan peraturan dan dasar keselamatan yang sedang berkuat kuasa. Sekiranya pembekal gagal mematuhi peraturan keselamatan tersebut, pihak Kerajaan berhak menghalang syarikat	Syarikat Pembekal/ Pemilik Projek / Bahagian Perolehan

ID	PENERANGAN	PERANAN
	pembekal daripada meneruskan penyampaian perkhidmatan. Perkara - perkara yang perlu dipatuhi: a. **Pendaftaran sah di bawah Kementerian Kewangan Malaysia** Pembekal hendaklah berdaftar secara sah dengan Kementerian Kewangan Malaysia (MOF) dalam Kod Bidang yang berkaitan. b. **Keutamaan kepada pembekal yang mempunyai pensijilan keselamatan** Pembekal yang mempunyai pensijilan keselamatan yang diiktiraf hendaklah diberi keutamaan dalam proses pemilihan. c. **Kelulusan keselamatan untuk wakil pembekal** Semua wakil pembekal yang terlibat dalam projek hendaklah mempunyai kelulusan keselamatan daripada agensi atau pihak berkuasa berkaitan. **d. Penilaian teknikal terhadap produk/ perkhidmatan** e. Produk atau perkhidmatan yang ditawarkan hendaklah melalui proses penilaian teknikal bagi memastikan pematuhan terhadap keperluan keselamatan. f. **Peranan Jawatankuasa Penilaian Teknikal (JPT)** JPT boleh melaksanakan penilaian teknikal sendiri atau membuat semakan terhadap laporan penilaian pihak ketiga yang dikemukakan oleh pembekal. g. **Semakan ke atas laporan pihak**	

ID	PENERANGAN	PERANAN
	ketiga Laporan penilaian keselamatan oleh pihak ketiga hendaklah disemak berdasarkan faktor berikut: i. Kebebasan dan integriti badan penilai; ii. Kompetensi badan penilai; iii. Kriteria penilaian yang digunakan; iv. Parameter pengujian; v. Andaian yang digunakan dalam penilaian dan skopnya. h. **Pemenuhan dokumen keselamatan berkaitan** Pembekal hendaklah bersetuju dan mematuhi keperluan keselamatan berikut: i. **Lampiran D:** Perjanjian Tidak Mendedahkan Maklumat (*Non-Disclosure Agreement*); ii. Lampiran E: Perakuan Akta Rahsia Rasmi 1972 (Akta 88). iii. Pemakaian pengkelasan maklumat Pembekal hendaklah mematuhi pengkelasan maklumat seperti yang telah ditetapkan oleh KPN/Agensi.	

5.21 Pengurusan Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat dan Komunikasi *(Managing information security in the information and communication technology (ICT) supply chain)*

ID	PENERANGAN	PERANAN
5.21.1	KPN/Agensi perlu memastikan keselamatan maklumat terpelihara sepanjang rantaian bekalan ICT, termasuk dalam pemerolehan, pembangunan, penghantaran, operasi dan penyelenggaraan perkhidmatan atau produk teknologi maklumat yang dibekalkan oleh pihak ketiga. Bagi memastikan keselamatan maklumat dalam perolehan dan penggunaan produk serta perkhidmatan ICT, perkara-perkara berikut hendaklah diberi perhatian: a. **Penetapan keperluan keselamatan maklumat** semasa perolehan ICT Keperluan keselamatan maklumat hendaklah ditentukan dan dimasukkan dalam spesifikasi teknikal, kontrak, atau dokumen perolehan berkaitan produk dan perkhidmatan ICT. b. **Pengurusan risiko keselamatan dalam rantaian pembekalan** Pembekal utama bertanggungjawab untuk mengenal pasti, menilai dan mengurus semua risiko keselamatan maklumat yang berkaitan dengan produk, perisian, perkhidmatan serta elemen dalam keseluruhan rantaian pembekalan. c. **Jaminan kebolehpercayaan pembekalan dan operasi** Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pemilik Projek dan Pembekal

5.22 Memantau, menyemak, menilai dan mengurus perubahan dalam perkhidmatan pembekal *(Monitoring, Review and Change Management of Supplier Services)*

ID	PENERANGAN	PERANAN
5.22.1	Memastikan pemantauan, penilaian dan pengurusan perubahan dilaksanakan secara konsisten ke atas semua perkhidmatan yang disediakan oleh pihak ketiga bagi menjamin keselamatan maklumat dan pematuhan terhadap kontrak perkhidmatan. Perkara yang perlu diberi perhatian adalah seperti berikut: **a. Pemantauan pematuhan terhadap kontrak perkhidmatan** Memastikan tahap perjanjian perkhidmatan pihak ketiga selaras dengan kontrak perjanjian. b. **Pemantauan dan pelaporan status perkhidmatan** Laporan perkhidmatan daripada pihak ketiga hendaklah dipantau dan status pelaksanaan dikemukakan kepada KPN/Agensi secara berkala. c. **Pengurusan insiden keselamatan maklumat** Pihak ketiga hendaklah dimaklumkan serta-merta sekiranya berlaku sebarang insiden keselamatan maklumat, dan bertanggungjawab untuk mengemukakan maklumat lanjutan serta tindakan susulan sebagaimana yang dinyatakan dalam kontrak perkhidmatan. d. **Tindakan ke atas insiden keselamatan** Insiden keselamatan maklumat yang dikenal pasti hendaklah ditangani segera melalui tindakan pembetulan dan pencegahan yang sewajarnya.	Pemilik Projek Pentadbir Sistem Aplikasi

ID	PENERANGAN	PERANAN
	e. **Pengurusan kelemahan keselamatan** Sebarang kelemahan keselamatan yang dikenal pasti dalam perkhidmatan/produk, sistem atau proses hendaklah dinilai dan ditangani dengan sewajarnya mengikut tahap risiko. f. **Tindakan ke atas ketidakpatuhan kontrak** Pihak ketiga yang didapati tidak memenuhi keperluan kontrak perjanjian boleh dikenakan tindakan bersesuaian seperti penalti.	
5.22.2	**Menguruskan Perubahan Kepada Perkhidmatan Pembekal *(Managing Changes To Supplier Services*** Perubahan perkhidmatan pihak ketiga hendaklah dilaksanakan secara teratur dan mengikut *Standard Operating Procedure* (SOP) yang ditetapkan. Perkara-perkara berikut hendaklah diambil kira adalah seperti berikut: a. Memastikan perubahan dalam perkhidmatan pihak ketiga dipersetujui bersama dan menguntungkan bagi pihak kerajaan. b. Memastikan perubahan dalam perjanjian dengan pihak ketiga mengambil kira maklumat kritikal KPN/Agensi , sistem serta proses yang terlibat dan kajian risiko. c. Pemantauan dan persetujuan ke atas perubahan perkhidmatan pihak ketiga hendaklah merangkumi perkara-perkara berikut:	Pemilik Projek / Pentadbir Sistem/ Sistem Aplikasi

ID	PENERANGAN	PERANAN
	i. Peningkatan kepada perkhidmatan/produk sedia ada termasuk rangkaian, perisian,versi dan alatan pembangunan. ii. Pembangunan sebarang aplikasi dan sistem baharu, iii. Pengubahsuaian atau kemaskini polisi dan prosedur pihak ketiga; iv. Kaedah kawalan baharu atau yang dikemaskini bagi keselamatan maklumat dan meningkatkan keselamatan maklumat; dan v. Perubahan lokasi perkhidmatan dan subkontraktor.	

5.23 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Pengkomputeran Awan *(Information Security for Use of Cloud Computing Services)*

ID	PENERANGAN	PERANAN
5.23.1	Bagi memastikan keselamatan maklumat sentiasa terpelihara dalam penggunaan perkhidmatan pengkomputeran awan, KPN/Agensi hendaklah melaksanakan perkara-perkara berikut: a. **Menentukan dan Mengurus Keselamatan Maklumat** i. Memastikan keselamatan maklumat dikawal dengan berkesan sepanjang kitaran hayat penggunaan perkhidmatan awan *(cloud)* ; termasuk pemerolehan, penggunaan, penyimpanan data serta penamatan perkhidmatan.	ICTSO/ BTM/ Ketua Agensi/ Pengguna

ID	PENERANGAN	PERANAN
	ii. Menjamin keutuhan, kerahsiaan dan ketersediaan data serta mencegah pencerobohan, kebocoran atau penyalahgunaan maklumat oleh pihak yang tidak berautoriti. **b. Pematuhan kepada Dasar dan Garis Panduan Terkini** i. Memastikan semua penggunaan dan pengurusan perkhidmatan pengkomputeran awan *(cloud)* mematuhi keperluan perundangan, peraturan, garis panduan serta syarat kontrak yang berkuat kuasa. **ii.** Ini termasuk pengurusan perkhidmatan oleh pembekal seperti yang diperincikan dalam pengurusan pihak ketiga **(rujuk Seksyen 5.21 dan 5.22).** **c. Pengurusan Risiko** Menentu/mentakrif dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan. d. **Pelaksanaan Kawalan Keselamatan Maklumat** Memastikan kawalan keselamatan maklumat dilaksanakan dalam setiap penggunaan perkhidmatan awan *(cloud),* termasuk pemantauan capaian, log audit dan enkripsi data. e. **Pengurusan Langganan dan Pematuhan Perisian** Melaksanakan kawalan terhadap keperluan langganan agar hanya perisian berlesen yang sah digunakan, serta pematuhan terhadap had	

ID	PENERANGAN	PERANAN
	pengguna yang telah ditetapkan atau dibenarkan. f. **Rujukan kepada Dasar dan Garis Panduan Semasa** Pengurusan keselamatan perkhidmatan pengkomputeran awan hendaklah berpandukan kepada dasar dan garis panduan semasa yang berkuat kuasa, termasuk: i. **PK 2.6 (15 April 2022)** Pekeliling Perbendaharaan Malaysia mengenai Perolehan Perkhidmatan Pengkomputeran Awan melalui *Cloud Framework Agreement* bagi Agensi Sektor Awam ii. **PKPA Bil. 1/2021 (10 Jun 2021)** Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam, menyokong inisiatif MyDigital dan penggunaan awan amanah kerajaan (seperti MyGovCloud@PDSA) iii. **Surat Pekeliling Am (SPA) Bil. 2/2021 (9 Ogos 2021), versi 2.0** Garis panduan kini dikemas kini (versi 2.0) untuk pengurusan keselamatan maklumat melalui pengkomputeran awan sektor awam iv. **ISO/IEC 27002:2022 (terbitan 15 Feb 2022)** Kod amalan keselamatan maklumat yang terkini; menggantikan versi 2013 v. **ISO/IEC 27017:2015** Kod amalan keselamatan maklumat khusus untuk perkhidmatan awan	

ID	PENERANGAN	PERANAN
	vi. **ISO/IEC 27018:2019** Kod amalan perlindungan data peribadi (PII) dalam awan awam	

5.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat *(Information Security Incident Management Planning and Preparation)*

ID	PENERANGAN	PERANAN
5.24.1	**Tanggungjawab Dan Prosedur *(Responsibilities And Procedures)*** Tanggungjawab dan prosedur pengurusan pengendalian insiden hendaklah mempunyai maklum balas yang cepat, berkesan dan teratur terhadap insiden. Pengurusan insiden KPN/Agensi hendaklah berdasarkan kepada Prosedur Operasi Standard (SOP) yang berkuat kuasa. Antara perkara yang perlu dilaksanakan adalah seperti yang berikut: a. Memberi kesedaran dan pemahaman secara berkala kepada warga kerja mengenai SOP berkaitan pengurusan insiden keselamatan siber (CSIRT) yang digunapakai. b. Memastikan personel yang terlibat dalam pengurusan insiden mempunyai kemahiran dan pengetahuan yang mencukupi untuk melaksanakan tugas mereka dengan berkesan.	ICTSO, Pengurus ICT, CSIRT Agensi, dan Pemilik Projek/ Sistem Aplikasi
5.24.2	**Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat *(Information Security Incident Management Planning and Preparation)*** Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenal pasti semua jenis insiden	ICTSO/ CSIRT Agensi

ID	PENERANGAN	PERANAN
	yang boleh mengancam keselamatan sistem. Ini termasuk gangguan perkhidmatan yang dilakukan secara sengaja, pemalsuan identiti pengguna bagi tujuan akses tanpa kebenaran, serta sebarang tindakan mengubah suai atau memasang perisian tanpa kebenaran. b. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti. c. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan. d. Menyediakan tindakan pemulihan segera. e. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan. f. Menyediakan tindakan pemulihan segera. g. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu. h. Sebaik sahaja insiden itu berjaya ditangani, ia hendaklah ditutup secara rasmi dan direkodkan.	

5.25 Penilaian dan Keputusan mengenai Peristiwa Keselamatan Maklumat *(Assessment of and Decision on Information Security Events)*

ID	PENERANGAN	PERANAN
5.25.1	Peristiwa Keselamatan Maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Ia hendaklah direkodkan sebagaimana Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan Siber Kementerian Perpaduan Negara dan Agensi.	ICTSO, pemilik sistem, pentadbir sistem & CSIRT Agensi

5.26 Pembelajaran Daripada Insiden Keselamatan Maklumat *(Learning from Information Security Incidents)*

ID	PENERANGAN	PERANAN
5.26.1	Pembelajaran daripada insiden keselamatan maklumat penting untuk mencegah kejadian yang sama berulang. Setiap insiden perlu di analisis bagi mengenal pasti punca, kelemahan sistem dan tindakan yang tidak berkesan. Maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk memperbaiki dan memperkukuh langkah-langkah keselamatan organisasi. Antaranya termasuk: a. Menambah baik pelan pengurusan insiden dengan mengemaskini senario dan prosedur berdasarkan insiden yang pernah berlaku. b. Mengenal pasti insiden yang berulang atau serius serta puncanya untuk dikaitkan dengan penilaian risiko semasa dan seterusnya menentukan kawalan	ICTSO, CSIRT

ID	PENERANGAN	PERANAN
	tambahan bagi mengurangkan risiko yang sama daripada berulang. c. Mengumpul dan menganalisis maklumat seperti jenis kejadian, kekerapan berlaku dan impak kos, bagi menilai keberkesanan tindakan dan membuat perancangan yang lebih baik. d. Meningkatkan kesedaran dan latihan kepada pengguna dengan menggunakan contoh kejadian sebenar sebagai panduan tentang apa yang perlu dilakukan dan bagaimana untuk mengelakkan insiden serupa di masa hadapan.	

5.27 Pengumpulan Bahan Bukti *(Collection of Evidence)*

Mengumpul dan menyimpan bahan bukti berkaitan insiden keselamatan maklumat dengan cara yang sah dan teratur untuk tujuan siasatan atau tindakan undang-undang.

ID	PENERANGAN	PERANAN
5.27.1	Dalam pengurusan insiden keselamatan maklumat, proses pengumpulan bahan bukti perlu dilaksanakan secara teliti dan mengikut prosedur bagi memastikan integriti, ketulenan, dan kebolehterimaan bahan bukti tersebut jika diperlukan untuk siasatan lanjut atau tindakan undang-undang. KPN/Agensi hendaklah: a. Mengumpul, merekod, menyalin dan menyimpan bahan bukti berkaitan insiden. b. Memastikan proses pengendalian	ICTSO, CSIRT Agensi

ID	PENERANGAN	PERANAN
	bukti mematuhi prinsip rantaian bukti *(chain of custody)* bagi menjamin bahan bukti tidak diubah, rosak atau hilang. c. Hanya personel yang terlatih dan berkemahiran dalam bidang forensik digital dibenarkan untuk mengendalikan bahan bukti. d. Menyimpan bahan bukti dalam persekitaran yang selamat dan dikawal aksesnya.	

5.28 Keselamatan Maklumat Semasa Gangguan *(Information Security During Disruption)*

ID	PENERANGAN	PERANAN
5.28.1	Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah yang diambil untuk melindungi data, sistem dan maklumat penting semasa berlaku gangguan seperti bencana alam, serangan siber, kebakaran, banjir atau kerosakan teknikal. Bagi memastikan maklumat kekal terpelihara, KPN/Agensi perlu mengambil tindakan seperti berikut: **a. Pelan Perancangan Kesinambungan Perkhidmatan (BCP)** Menyediakan perancangan strategik untuk memastikan operasi penting terus berjalan walaupun dalam keadaan gangguan besar. **b. Pelan Pemulihan Bencana**	Pentadbir Rangkaian/ Pentadbir Sistem/ Pegawai KPN/Agensi / Pihak Ketiga

ID	PENERANGAN	PERANAN
	(DRP) Menetapkan proses dan langkah teknikal untuk memulihkan sistem aplikasi dan data yang terjejas selepas bencana. **c. Perlindungan Data *(Data Protection)*** Melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data yang sensitif. **d. Langkah Pencegahan Serangan Siber *(Cybersecurity)*** Melibatkan tindakan untuk mencegah serangan siber dan melindungi data dari ancaman siber. ***e.* Pemulihan Sistem Cepat *(Quick Recovery)*** i. Penggunaan sistem pemulihan automatik atau sandaran segera ii. Pemantauan masa nyata untuk mengurangkan waktu henti sistem *iii.* Kesedaran Keselamatan (*Security Awareness)* iv. Latihan dan kempen keselamatan berkala kepada warga v. Simulasi insiden keselamatan untuk kesediaan dalaman f. **Pelan Komunikasi Krisis *(Crisis Communication Plan)*** yang jelas untuk mengurus krisis dan insiden dengan pantas.	

ID	PENERANGAN	PERANAN
	Keselamatan maklumat semasa gangguan adalah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan organisasi mampu menjaga integriti, kerahsiaan, dan ketersediaan maklumat penting dalam pelbagai situasi yang mengancam.	

5.29 Kesediaan ICT Bagi Kesinambungan Perkhidmatan *(ICT Readiness for Business Continuity)*

ID	PENERANGAN	PERANAN
5.29.1	Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji secara berkala bagi memastikan kesinambungan perkhidmatan organisasi sekiranya berlaku gangguan. Bagi mencapai objektif ini, KPN/Agensi hendaklah memastikan perkara-perkara berikut: a. **Struktur Organisasi yang Mencukupi** Organisasi perlu mewujudkan struktur yang jelas dan mencukupi bagi menyokong penyediaan, pengurangan impak, serta tindakan balas terhadap sebarang gangguan perkhidmatan ICT. Struktur ini hendaklah disokong oleh pegawai yang mempunyai tanggungjawab, kuasa dan tahap kecekapan yang bersesuaian. **b. Pelan Kesinambungan Perkhidmatan atau Pelan Pemulihan Bencana (BCP/DRP)** Organisasi hendaklah menyediakan Pelan Kesinambungan Perkhidmatan	CDO, ICTSO & CSIRT

ID	PENERANGAN	PERANAN
	atau Pelan Pemulihan Bencana (BCP/DRP) yang mengandungi langkah-langkah tindakan dan pemulihan sekiranya berlaku gangguan ICT. Pelan ini hendaklah: i. **Diluluskan** oleh pihak pengurusan tertinggi; ii. **Diuji dan dinilai** secara berkala melalui latihan atau simulasi untuk memastikan pelaksanaannya berkesan dan relevan. c. **Kandungan Pelan BCP/DRP** Pelan BCP/DRP hendaklah merangkumi perkara berikut: i. Spesifikasi prestasi dan kapasiti perkhidmatan ICT, yang memenuhi keperluan dan objektif kesinambungan perkhidmatan sebagaimana ditentukan dalam Analisis Impak Perniagaan *(Business Impact Analysis,* BIA); ii. Objektif Masa Pemulihan *(Recovery Time Objective*, RTO) bagi setiap perkhidmatan ICT yang kritikal, termasuk prosedur pemulihan bagi komponen berkaitan; iii. Objektif Titik Pemulihan (*Recovery Point Objective,* RPO) yang menetapkan had maksimum kehilangan data yang boleh diterima untuk setiap sumber ICT.	

ID	PENERANGAN	PERANAN
5.29.2	**Kesinambungan Keselamatan Maklumat dalam Pengurusan Kesinambungan Perkhidmatan (BCMS)** Keselamatan maklumat hendaklah diterapkan dalam Sistem Pengurusan Kesinambungan Perkhidmatan (BCMS) di peringkat KPN/Agensi. KPN/Agensi hendaklah menentukan keperluan keselamatan maklumat dan memastikan kesinambungan pengurusan keselamatan maklumat dapat dikekalkan dalam situasi kecemasan seperti krisis, bencana atau gangguan besar terhadap operasi. Dalam perancangan kesinambungan keselamatan maklumat, KPN/Agensi perlu mengambil kira: i. Isu dalaman dan luaran yang boleh memberi kesan kepada penyampaian perkhidmatan dan fungsi utama organisasi; *ii.* Keperluan serta jangkaan pihak berkepentingan *(stakeholders);* iii. Keperluan undang-undang, peraturan dan garis panduan yang berkaitan. Perkara-perkara yang Perlu Dipertimbangkan Bagi memastikan kesinambungan keselamatan maklumat yang berkesan, KPN/Agensi hendaklah melaksanakan langkah-langkah berikut: a. **Melantik Pasukan Tadbir Urus Pengurusan**	Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT (ICTSO & CSIRT)

ID	PENERANGAN	PERANAN
	Kesinambungan Perkhidmatan (PKP) Pasukan ini bertanggungjawab merancang, melaksana dan memantau aktiviti kesinambungan perkhidmatan dan keselamatan maklumat. b. **Menetapkan Polisi PKP** Polisi ini hendaklah menggariskan prinsip, peranan dan tanggungjawab berkaitan pengurusan kesinambungan perkhidmatan dan keselamatan maklumat. c. **Mengenal Pasti Perkhidmatan Kritikal** Perkhidmatan yang memberi kesan besar kepada operasi organisasi sekiranya terganggu perlu dikenal pasti dan diberi keutamaan dalam pelan kesinambungan. **d. Melaksanakan Kajian Impak Perkhidmatan *(Business Impact Analysis* – BIA) dan Penilaian Risiko** Kajian ini bertujuan untuk mengenal pasti kesan gangguan serta risiko terhadap perkhidmatan kritikal dan keselamatan maklumat **e. Membangunkan Dokumen-dokumen Sokongan ;** i. Pelan Induk Pengurusan Kesinambungan Perkhidmatan (BCMP); ii. Pelan Komunikasi Krisis;	

ID	PENERANGAN	PERANAN
	iii. Pelan Tindak Balas Kecemasan; iv. Pelan Pemulihan Bencana ICT *(Disaster Recovery Plan* – DRP). f. **Melaksanakan Program Kesedaran dan Latihan** Program latihan berkala perlu diberikan kepada pasukan PKP dan pengguna organisasi bagi memastikan kesiapsiagaan dan keberkesanan pelaksanaan pelan. **g. Melaksanakan Simulasi dan Penyenggaraan Pelan** Ujian simulasi dan semakan berkala terhadap pelan-pelan berkaitan hendaklah dijalankan bagi memastikan pelan sentiasa dikemas kini dan bersesuaian dengan keperluan semasa.	
5.29.3	**Pelaksanaan Pelan Kesinambungan Perkhidmatan (PKP)** KPN/Agensi hendaklah memastikan proses, prosedur dan kawalan keselamatan maklumat dilaksanakan dengan sewajarnya bagi menjamin tahap keselamatan yang diperlukan ketika gangguan berlaku. Tindakan yang perlu diambil termasuk: a. Melaksanakan pelan PKP apabila berlaku gangguan terhadap perkhidmatan kritikal. b. Melaksanakan *post-mortem* selepas pelaksanaan PKP bagi menilai keberkesanan tindak balas.	Koordinator PKP Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT

ID	PENERANGAN	PERANAN
	c. Mengemas kini pelan sekiranya berlaku perubahan ketara dalam organisasi, teknologi atau sumber. d. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan masing-masing.	
5.29.4	**Pengesahan, Kajian Semula dan Penilaian Kesinambungan Keselamatan Maklumat *(Verify, Review and Evaluate Information Security Continuity)*** Bagi memastikan kawalan keselamatan maklumat yang berkaitan kesinambungan sentiasa relevan dan berkesan, KPN/Agensi hendaklah melaksanakan tindakan berikut secara sistematik dan berkala: **a. Pengesahan *(Verification)*** i. Menyemak pelaksanaan kawalan keselamatan maklumat bagi memastikan ia mematuhi pelan yang telah dirancang; dan ii. Menilai pematuhan terhadap polisi, prosedur dan pelan kesinambungan. b. **Kajian Semula *(Review)*** i. Menilai dokumen utama seperti BCP, DRP dan Pelan Tindak Balas Kecemasan; dan ii. Kajian semula perlu mengambil kira perubahan dalam teknologi, persekitaran operasi dan perundangan.	Pengurusan Atasan KPN/Agensi , Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT, Pemilik Perkhidmatan Kritikal Agensi dalam PKP dan warga KPN/Agensi

ID	PENERANGAN	PERANAN
	c. **Penilaian *(Evaluation)*** i. Menilai keberkesanan kawalan melalui audit dalaman, latihan simulasi dan penilaian risiko; ii. Mendokumenkan hasil penilaian dan melaksanakan tindakan penambahbaikan ke atas sebarang kelemahan atau jurang yang dikenal pasti.	
5.29.5	Perkara yang perlu diambil kira adalah seperti berikut: a. Membangunkan Analisis Bisnes Impak (BIA) dengan mengenal pasti Aset ICT yang terlibat; b. Mengenal pasti *Recovery Time Objective* (RTO) dan *Recovery Point Objective* (RPO) untuk sistem aplikasi kritikal mengikut keutamaan; c. Menyediakan Pelan Pemulihan Bencana ICT (DRP) dan memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab; d. Menjalankan pengujian bagi memastikan ketersediaan Aset ICT dapat berfungsi semasa gangguan; dan e. Senarai lengkap maklumat yang memerlukan backup dan lokasi penyimpanannya.	Pasukan DRP

5.30 Keperluan Perundangan dan *Kontrak (Legal, Statutory, Regulatory and Contractual Requirements)*

ID	PENERANGAN	PERANAN
5.30.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak *(Compliance with Legal and Contractual Requirements)*** KPN/Agensi , termasuk semua warga kerja serta pihak ketiga seperti kontraktor, subkontraktor dan perunding, hendaklah mematuhi sepenuhnya semua keperluan yang ditetapkan dalam perundangan, peraturan, perjanjian kontrak dan dasar organisasi yang berkuat kuasa dari semasa ke semasa. Sebarang pelanggaran terhadap klausa dalam dokumen perundangan atau kontrak, termasuk *"Integrity Pact"*, adalah dianggap sebagai pelanggaran serius dan boleh menyebabkan: a. Penamatan kontrak atau perkhidmatan serta-merta. b. Tindakan undang-undang atau tatatertib yang bersesuaian. c. Pelaporan kepada pihak berkuasa yang berkaitan jika melibatkan pelanggaran jenayah atau integriti. **Senarai Rujukan Perundangan dan Peraturan** Semua pegawai dan petugas KPN/Agensi perlu memastikan pematuhan terhadap perundangan dan peraturan seperti berikut (tidak terhad kepada): a. Akta Suruhanjaya Komunikasi dan Multimedia Malaysia 1998 (Akta	Entiti Berkaitan/ Pihak Ketiga KPN/Agensi

ID	PENERANGAN	PERANAN
	589) b. Akta Rahsia Rasmi 1972 (Akta 88) c. Akta Perlindungan Data Peribadi 2010 (Akta 709) d. Akta Jenayah Komputer 1997 (Akta 563); e. Arahan Keselamatan (dikeluarkan oleh MKN) f. Garis Panduan Keselamatan Siber Kerajaan Malaysia Pekeliling Perkhidmatan, Arahan Perbendaharaan dan surat pekeliling yang berkaitan ICT dan keselamatan maklumat. **Tanggungjawab Pematuhan** a. Semua pegawai dan warga adalah bertanggungjawab untuk memahami dan mematuhi undang-undang serta peraturan yang berkaitan dalam pelaksanaan tugasan mereka. b. Pasukan ICT dan Keselamatan Maklumat hendaklah memantau dan mengemas kini senarai keperluan perundangan dari semasa ke semasa serta memberi panduan kepada warga organisasi. c. Pegawai yang bertanggungjawab terhadap pengurusan kontrak hendaklah memastikan bahawa sebarang perjanjian dengan pihak ketiga memasukkan klausa keselamatan maklumat dan pematuhan perundangan yang relevan.	

ID	PENERANGAN	PERANAN
5.30.2	**Pengenalpastian Keperluan Undang-Undang dan Kontrak yang Terpakai *(Identification of Applicable Legislation and Contractual Agreement)*** KPN/Agensi hendaklah mengenal pasti serta memastikan pematuhan terhadap semua keperluan undang-undang, peraturan dan perjanjian kontrak yang dipakai oleh warga kerja, pengguna, pembekal, pakar runding dan mana-mana pihak yang terlibat dalam perkhidmatan ICT. Senarai keperluan ini termasuk undang-undang dan peraturan berkaitan keselamatan maklumat yang berkuat kuasa dari semasa ke semasa dan perlu dipatuhi sepenuhnya oleh semua pihak yang berurusan dengan sistem dan maklumat KPN/Agensi .	Warga KPN/Agensi, pakar runding, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi
5.30.3	**Peraturan Kawalan Kriptografi (*(Regulation of Cryptographic Controls)*** Kriptografi ialah kaedah penyulitan data yang digunakan untuk memastikan hanya pihak yang sah dan diberi kuasa sahaja boleh membaca atau mengakses maklumat tersebut. Pengurusan kunci kriptografi yang digunakan untuk melindungi maklumat kritikal atau sensitif hendaklah dilaksanakan dengan cekap dan selamat, bagi mengelakkan kunci tersebut daripada diubah, dimusnahkan atau didedahkan tanpa kebenaran sepanjang tempoh kesahannya. Antara kawalan yang perlu dilaksanakan termasuklah:	Warga KPN/Agensi, pakar runding, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi

ID	PENERANGAN	PERANAN
	a. Kesemua pelaksanaan sistem hendaklah menggunakan ID atau kata laluan yang dilindungi melalui kaedah penyulitan (*encrypted*). b. Menggunakan *Public Key Infrastructure* (PKI) yang selamat dan dibekalkan oleh pihak Kerajaan. c. Kawalan kriptografi mestilah digunakan mengikut semua perjanjian, undang-undang dan peraturan yang sedang berkuat kuasa. Antara perkara yang perlu dipatuhi adalah: a. Sekatan import dan eksport terhadap perkakasan atau perisian komputer yang mempunyai fungsi kriptografi. b. Sekatan import dan eksport terhadap perkakasan atau perisian yang diubah suai atau direka khas untuk menjalankan fungsi kriptografi. c. Sekatan ke atas penggunaan enkripsi. d. Kaedah akses oleh pihak berkuasa Malaysia mengenai maklumat enkripsi perkakasan dan perisian.	

5.31 Hak Harta Intelek *(Intellectual Property Rights)*

ID	PENERANGAN	PERANAN
5.32.1	Memastikan kepatuhan terhadap keperluan perundangan,peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga KPN/Agensi , pakar runding, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi
5.32.1	KPN/Agensi perlu memastikan semua pihak mematuhi undang-undang, peraturan serta perjanjian kontrak berkaitan hak harta intelek. Ini termasuk: a. Menggunakan perisian yang mempunyai lesen yang sah. b. Mematuhi had bilangan pengguna yang dibenarkan dalam lesen perisian. c. Mengelakkan penggunaan bahan atau perisian tanpa kebenaran. **Tanggungjawab Warga KPN/Agensi dan Pihak Ketiga**. Semua pengguna sistem maklumat termasuk warga dan pihak ketiga perlu: a. Mengiktiraf dan menghormati hak cipta bagi bahan, perisian dan rekabentuk yang dimiliki atau diperoleh oleh KPN/Agensi. b. Mengikuti syarat pelesenan, termasuk batasan penggunaan	Warga KPN/Agensi/ Pihak Ketiga

ID	PENERANGAN	PERANAN
	produk, perisian, rekabentuk, dan bahan lain. c. Mematuhi sekatan hak cipta dan lesen pada setiap masa. d. Tidak menggunakan kemudahan ICT KPN/Agensi untuk tujuan yang tidak dibenarkan atau melanggar hak cipta.	

5.32 Perlindungan Rekod *(Protection of Records)*

ID	PENERANGAN	PERANAN
5.32.1	**Perlindungan Rekod *(Protection of Records)*** Semua rekod rasmi kerajaan hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa kebenaran, serta pendedahan kepada individu atau entiti yang tidak berkenaan. Perlindungan ini hendaklah dilaksanakan selaras dengan peruntukan undang-undang, peraturan pentadbiran, kontrak, serta garis panduan keselamatan maklumat dan pengurusan rekod yang berkuat kuasa. **Keperluan Perlindungan Rekod:** **a. Klasifikasi Rekod** Semua dokumen dan rekod perlu diklasifikasikan dan dilabelkan mengikut tahap keselamatan yang ditetapkan, iaitu **Terbuka, Terhad, Sulit, Rahsia**, atau **Rahsia Besar**, seperti yang ditetapkan dalam **Arahan Keselamatan**.	Warga KPN/Agensi , pakar runding, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi

ID	PENERANGAN	PERANAN
	b. Pengendalian dan Pergerakan Dokumen Semua pergerakan dokumen atau fail hendaklah direkodkan dan dikendalikan mengikut **Prosedur Keselamatan Dokumen** yang ditetapkan oleh KPN/Agensi, termasuk kawalan akses fizikal dan log digital. c. **Pelaporan Insiden Rekod** Sebarang kehilangan, kerosakan atau kebocoran maklumat dalam dokumen perlu dilaporkan segera kepada pihak berkuasa berkenaan, mengikut **Arahan Keselamatan** dan **Garis Panduan Notifikasi Pelanggaran Data *(Data Breach Notification Guideline,* PDPA, 2025)**. i. Notifikasi kepada Pesuruhjaya PDPC hendaklah dibuat dalam tempoh **72 jam** selepas insiden diketahui.Sekiranya terdapat risiko terhadap subjek data, mereka hendaklah dimaklumkan dalam masa **7 hari**. d. **Pelupusan Rekod** Pelupusan dokumen perlu dilaksanakan mengikut keperluan terkini dalam: ii. Panduan Pengurusan Rekod Sektor Awam (Arkib Negara Malaysia, 2024)	

ID	PENERANGAN	PERANAN
	iii. Panduan Pengurusan Rekod Sektor Awam (Arkib Negara Malaysia, 2024) iv. Jadual Pelupusan Rekod (JPR) yang diluluskan; v. Arahan Keselamatan dan tatacara yang diluluskan oleh Arkib Negara Malaysia. e. **Pemindahan Data ke Luar Negara** Sekiranya terdapat keperluan untuk memindahkan data atau rekod ke luar negara, KPN/Agensi hendaklah: *i.* Melaksanakan ***Transfer Impact Assessment*** **(TIA)** ii. Mematuhi **Garis Panduan Pemindahan Data Peribadi Rentas Sempadan (PDPD, 2025)** iii. Mendapat kelulusan pentadbiran dan memastikan kontrak standard (*Standard Contractual Clauses)* digunakan jika perlu. iv. **Keselamatan Rekod Digital** Dokumen atau rekod yang mengandungi maklumat rasmi dan dihantar secara elektronik hendaklah v. Dilindungi menggunakan **enkripsi (*encrypted*)**	

ID	PENERANGAN	PERANAN
	vi. Disimpan dalam sistem yang mematuhi kawalan akses berasaskan peranan *(Role-Based Access Control*, RBAC) vii. Menggunakan Server atau infrastruktur yang mematuhi dasar **keselamatan siber nasional** dan **SPRM (Standard Perlindungan Rangkaian dan Maklumat)** **Rujukan :** i. Akta Perlindungan Data Peribadi (Pindaan) 2024, mula berkuatkuasa 1 Jun 2025 ii. Garis Panduan Notifikasi Pelanggaran Data, Pesuruhjaya PDPD, 2025 iii. Garis Panduan Pemindahan Data Rentas Sempadan, PDPD, 2025 iv. Akta Perkongsian Data 2025 v. Panduan Pengurusan Rekod Sektor Awam, Arkib Negara Malaysia, Edisi 2024 vi. Arahan Keselamatan Malaysia (terkini)	

5.33 Privasi dan Perlindungan Peribadi yang boleh dikenal pasti *(Privacy and protection of personal identifiable information (PII))*

ID	PENERANGAN	PERANAN
5.33.1	Maklumat Peribadi yang Boleh Dikenal Pasti *(Personally Identifiable Information* - PII) merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti seseorang individu, sama ada secara langsung atau tidak langsung. Contoh maklumat PII termasuk tetapi tidak terhad kepada nombor kad pengenalan, alamat, nombor telefon, maklumat kesihatan, rekod kewangan, atau butiran biometrik. Garis Panduan Perlindungan PII adalah seperti berikut: **a. Persetujuan Individu** Sebarang pengumpulan, penggunaan, penyimpanan atau pendedahan maklumat peribadi hendaklah dilakukan dengan mendapatkan persetujuan terlebih dahulu daripada individu yang berkaitan. **b. Tanggungjawab Organisasi** KPN/Agensi bertanggungjawab untuk memastikan semua maklumat peribadi dikendalikan dengan selamat dan tidak didedahkan kepada pihak yang tidak berkenaan. c. **Akses Terhad dan Terurus** Akses kepada maklumat peribadi hendaklah dihadkan kepada pegawai yang diberi kuasa sahaja, dan mengikut keperluan tugasan.	Warga KPN/Agensi , pakar runding, pembekal, dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi

ID	PENERANGAN	PERANAN
	d. **Keselamatan Maklumat Digital** Maklumat peribadi yang disimpan atau dihantar secara elektronik hendaklah dilindungi menggunakan langkah keselamatan seperti kawalan akses, kata laluan, dan enkripsi. e. **Penyimpanan dan Pelupusan Selamat** Semua maklumat peribadi hendaklah disimpan dengan selamat dan dilupuskan mengikut tatacara yang ditetapkan apabila tidak lagi diperlukan. f. **Kerahsiaan dan Integriti Data** Segala maklumat peribadi hendaklah dilindungi daripada kehilangan, kerosakan, pemalsuan atau akses tanpa kebenaran bagi menjamin kerahsiaan dan integriti data.	
5.33.2	KPN/Agensi bertanggungjawab untuk memastikan bahawa semua maklumat peribadi pengguna dilindungi sepenuhnya, mengikut garis panduan, dasar, dan peraturan yang ditetapkan oleh pihak berkuasa yang berwibawa di Malaysia.	ICTSO

5.34 Kajian Semula Keselamatan Maklumat Secara Berkecuali *(Independent Review of Information Security)*

ID	PENERANGAN	PERANAN
5.34.1	**Kajian Keselamatan Maklumat Secara Berkala *(Independent Review of Information Security)*** Kajian keselamatan maklumat secara berkala hendaklah dilaksanakan bagi menilai tahap keberkesanan dan kecekapan sistem pengurusan keselamatan maklumat yang digunapakai oleh KPN/Agensi . Tujuan utama kajian ini adalah untuk memastikan bahawa kawalan keselamatan yang dilaksanakan: a. Berfungsi dengan baik. b. Mematuhi dasar dan prosedur yang ditetapkan. c. Selaras dengan keperluan undang-undang, peraturan dan standard keselamatan maklumat yang berkaitan. Kajian ini boleh dilaksanakan oleh pihak dalaman yang bebas atau pihak ketiga yang diiktiraf, dan hendaklah dijalankan mengikut jadual yang ditetapkan secara berkala. Sebarang penemuan daripada kajian hendaklah direkodkan, dianalisis dan ditindaklanjuti dengan pelan tindakan pembetulan bagi menambah baik keselamatan maklumat secara berterusan.	SUB/ Pengurus ICT dan Pemilik Perkhidmatan
5.34.2	Kajian bebas terhadap pelaksanaan keselamatan maklumat KPN/Agensi perlu dilakukan secara berkala atau apabila berlaku perubahan besar, bagi memastikan ia terus berkesan dan relevan.	Jawatankuasa Pemandu

5.35 Pematuhan Dasar, Peraturan dan Piawaian Untuk Keselamatan Maklumat *(Compliance With Policies, Rules and Standards for Information Security)*

ID	PENERANGAN	PERANAN
5.35.1	**Tanggungjawab Pengguna** Setiap pengguna di KPN/Agensi bertanggungjawab untuk: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber (PKS). b. Mematuhi semua undang-undang, peraturan, dasar dan piawaian yang berkuat kuasa berkaitan keselamatan maklumat dan penggunaan ICT. **Semua aset ICT**, termasuk sistem, peralatan, perisian dan maklumat yang disimpan di dalamnya, adalah hak milik KPN/Agensi dan hanya boleh digunakan untuk tujuan rasmi yang dibenarkan. **KSU, KP atau pegawai yang diberi kuasa** berhak untuk memantau aktiviti pengguna bagi memastikan tiada penyalahgunaan. Sebarang penggunaan aset ICT selain daripada maksud dan tujuan yang ditetapkan akan dianggap sebagai **penyalahgunaan sumber organisasi** dan boleh dikenakan tindakan.	Pengurus ICT dan Pemilik Perkhidmatan
5.35.2	**Pematuhan Dasar dan Piawaian Keselamatan** KPN/Agensi hendaklah menjalankan kajian semula secara berkala terhadap pematuhan dasar, peraturan dan	CDO/ Pengurus ICT

ID	PENERANGAN	PERANAN
	piawaian keselamatan maklumat yang diguna pakai. Jika berlaku ketidakpatuhan, langkah-langkah berikut hendaklah diambil: a. Mengenal pasti punca ketidakpatuhan. b. Menilai keperluan tindakan untuk memulihkan pematuhan. c. Melaksanakan tindakan pembetulan yang sewajarnya. d. Mengkaji semula tindakan yang diambil untuk memastikan keberkesanan dan mengesan sebarang kelemahan yang masih wujud.	
5.35.3	**Kajian Semula Pematuhan Teknikal *(Technical Compliance Review)*** *ICT Security Officer* (ICTSO) hendaklah memastikan semua prosedur keselamatan yang berada di bawah kawalannya: a. Mematuhi dasar, piawaian dan keperluan teknikal yang ditetapkan. b. Disemak semula secara berkala untuk memastikan kesesuaian dengan perubahan teknologi atau keperluan keselamatan semasa. KPN/Agensi juga hendaklah menjalankan kajian pematuhan terhadap: a. Proses pemprosesan maklumat; dan	ICTSO, Setiausaha Bahagian (SUB) / Pengurus ICT dan Pemilik Perkhidmatan

ID	PENERANGAN	PERANAN
	b. Pelaksanaan prosedur ICT mengikut ketetapan dalam polisi, piawaian dan peraturan yang berkaitan.	

5.36 Dokumentasi Prosedur Operasi yang Didokumenkan *(Documented Operating Procedures)*

ID	PENERANGAN	PERANAN
5.36.1	**Pematuhan Dokumentasi Prosedur** Setiap prosedur operasi yang melibatkan keselamatan siber di KPN/Agensi hendaklah: a. Didokumenkan dengan lengkap, disimpan dan dikawal rapi; b. Merangkumi semua prosedur yang telah diwujudkan, dikenal pasti dan masih digunakan; c. Mengandungi arahan yang jelas, tersusun dan lengkap termasuk perkara berikut: i. Keperluan kapasiti sistem; ii. Pengendalian dan pemprosesan maklumat; iii. Pengurusan dan penghantaran ralat; iv. Pengendalian output; v. Bantuan teknikal; dan vi. Tindakan pemulihan sekiranya berlaku gangguan atau kegagalan pemprosesan. d. Dokumen prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau apabila berlaku perubahan keperluan operasi.	Pengurus ICT, Pentadbir Sistem, Pentadbir Rangkaian dan Keselamatan ICT serta Pentadbir Pusat Data

ID	PENERANGAN	PERANAN
5.36.2	**Penyediaan Prosedur Operasi** Dokumen operasi standard (SOP) hendaklah disediakan bagi situasi berikut: a. Aktiviti harian yang sentiasa dilaksanakan oleh warga KPN/Agensi ; b. Aktiviti yang jarang dilakukan; c. Aktiviti baharu yang belum dinilai dari segi risiko; dan d. Proses serahan tugas kepada warga baharu.	ICTSO/ Pentadbir Sistem Aplikasi
5.36.3	**Kandungan Dokumen Prosedur Operasi** Dokumen Prosedur Operasi hendaklah diwujudkan, disemak dan dikemaskini mengikut keperluan. Kandungannya perlu merangkumi: a. Pegawai yang bertanggungjawab terhadap pelaksanaan prosedur; b. Prosedur instalasi dan konfigurasi sistem; c. Pemprosesan maklumat secara manual dan automatik; d. Kaedah sandaran *(backup)* dan pemulihan data; Jadual operasi serta kebergantungan sistem; e. Pengendalian kesilapan dan ralat; Sokongan teknikal sekiranya berlaku masalah; f. Arahan pengendalian media storan; g. Prosedur pemulihan sistem sekiranya berlaku kegagalan; h. Pengurusan jejak audit sistem; i. Pemantauan kapasiti, prestasi dan keselamatan sistem; dan j. Manual penyelenggaraan sistem.	ICTSO/ Pentadbir Sistem Aplikasi

6 KAWALAN SUMBER MANUSIA

6.1 Tapisan

Memastikan pengguna di bawahnya dan pihak ketiga yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi memahami tanggungjawab dan peranan masing-masing, serta meningkatkan pengetahuan dalam aspek keselamatan aset ICT. Selaras dengan keperluan ini, semua pihak yang terlibat juga dikehendaki menjalani proses tapisan keselamatan sebagai langkah awal sebelum diberikan akses kepada sistem atau aset ICT berkaitan.

ID	PENERANGAN	PERANAN
6.1.1	Semakan dan pengesahan latar belakang hendaklah dilakukan ke atas semua pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi sebelum berurusan dengan KPN/Agensi . Tapisan ini perlu dilaksanakan secara awal dan berterusan, dengan mengambil kira undang-undang, peraturan serta etika yang berkuat kuasa. Pelaksanaannya hendaklah seimbang dan bersesuaian dengan: a. Keperluan operasi dan perniagaan; b. Tahap klasifikasi maklumat yang akan diakses; dan c. Risiko keselamatan yang mungkin timbul.	Pengguna dan Pihak Ketiga

6.2 Terma Dan Syarat Perjawatan

ID	PENERANGAN	PERANAN
6.2.1	Setiap pengguna hendaklah melaksanakan tanggungjawab dan peranan masing-masing dengan berdisiplin, meningkatkan pengetahuan dalam keselamatan aset ICT, serta mematuhi semua syarat perkhidmatan dan peraturan yang berkuatkuasa semasa melaksanakan tugasan rasmi harian.	Pengguna
6.2.2	Perjanjian kontrak pekerjaan hendaklah dengan jelas menyatakan tanggungjawab	Pengguna dan Pihak Ketiga

ID	PENERANGAN	PERANAN
	pengguna dan pihak ketiga dalam organisasi bagi memastikan keselamatan maklumat sentiasa dipelihara.	
6.2.3	Semua pengguna dan pihak ketiga hendaklah mematuhi terma dan syarat perkhidmatan yang ditetapkan serta mematuhi peraturan semasa yang berkuat kuasa di KPN/Agensi.	Pengguna dan Pihak Ketiga

6.3 Kesedaran, Pendidikan Dan Latihan Keselamatan Maklumat

ID	PENERANGAN	PERANAN
6.3.1	Pengguna dan pihak ketiga yang berkaitan hendaklah diberikan pendedahan berkala melalui program kesedaran, pendidikan atau latihan keselamatan maklumat yang bersesuaian. Latihan ini perlu merangkumi dasar, prosedur, dan topik-topik keselamatan maklumat yang berkaitan dengan tanggungjawab dan fungsi tugas masing-masing. Kemaskini maklumat keselamatan hendaklah disampaikan secara berterusan bagi memastikan pematuhan terhadap dasar keselamatan maklumat organisasi.	ICTSO, Pengguna dan Pihak ketiga

6.4 Proses Tatatertib/Tindakan Undang - Undang

ID	PENERANGAN	PERANAN
6.4.1	Prosedur tatatertib/tindakan undang-undang hendaklah dirangka secara formal dan dihebahkan kepada pengguna bagi membolehkan tindakan diambil terhadap mana-mana individu yang melanggar dasar keselamatan maklumat.	Pegawai Keselamatan ICT Kementerian/Agensi

ID	PENERANGAN	PERANAN
6.4.2	Sebarang pelanggaran terhadap Polisi Keselamatan Siber (PKS) boleh dikenakan tindakan tatatertib/ tindakan undang-undang mengikut tatacara pengurusan salah laku, tindakan tatatertib dan kesalahan jenayah seperti yang diperuntukkan dalam pekeliling dan peraturan Kerajaan yang berkuatkuasa.	

6.5 Tanggungjawab Selepas Penamatan Atau Perubahan Pengguna

ID	PENERANGAN	PERANAN
6.5.1	Bagi memastikan keselamatan dan integriti sistem serta aset ICT, semua urusan penamatan perkhidmatan pengguna yang bertukar, bersara atau tamat perkhidmatan hendaklah dilaksanakan secara teratur dan menurut prosedur yang ditetapkan. Perkara-perkara berikut hendaklah dipatuhi: a. **Pemulangan Aset ICT** Semua aset ICT yang telah dibekalkan hendaklah dikembalikan kepada KPN/Agensi mengikut peraturan serta terma perkhidmatan yang berkuat kuasa. b. **Pembatalan Capaian Sistem dan Maklumat** Segala kebenaran capaian ke atas sistem, maklumat, dan kemudahan pemprosesan maklumat hendaklah dibatalkan atau ditarik balik mengikut peraturan dan garis panduan keselamatan ICT yang telah ditetapkan oleh KPN/Agensi . c. **Pengurusan Aset ICT bagi Pengguna yang Bertukar Tempat Bertugas** Pengguna yang bertukar cawangan,	ICTSO, Pengguna dan Pihak ketiga

ID	PENERANGAN	PERANAN
	negeri atau bahagian tidak dibenarkan membawa bersama aset ICT ke tempat baharu, kecuali dengan kebenaran. d. **Pembersihan data bagi kontrak sewaan peralatan ICT** Pihak ketiga perlu melaksanakan kerja-kerja pembersihan data *(data sanitizing)* bagi peralatan ICT di bawah kontrak sewaan yang telah tamat merujuk kepada Surat Pekeliling Am Bilangan 4 – Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam.	

6.6 Perjanjian Kerahsiaan Atau Ketakdedahan

ID	PENERANGAN	PERANAN
6.6.1	Semua Pengguna dan Pihak Ketiga yang menguruskan maklumat terperinci hendaklah mematuhi semua peruntukan **Akta Rahsia Rasmi 1972 (Pindaan 1986)** dan **arahan rasmi (Surat Pekeliling Am 1987, pangkalan SPA 2024)**. Pihak ketiga yang menggunakan dan mengakses aset ICT KPN/Agensi mesti menandatangani **Surat Akuan Rahsia Rasmi 1972, Pelantikan Di Bawah Seksyen 2b** seperti di **Lampiran 1C** atau **C**.	Pengguna dan Pihak Ketiga

6.7 Kerja Jarak Jauh *(Remote Working)*

ID	PENERANGAN	PERANAN
6.7.1	Langkah-langkah keselamatan hendaklah dilaksanakan apabila warga bekerja dari lokasi luar premis KPN/Agensi bagi	Pengurus ICT dan Pengguna

ID	PENERANGAN	PERANAN
	memastikan maklumat yang diakses, diproses atau disimpan sentiasa dilindungi.	
6.7.2	Dasar dan langkah keselamatan sokongan perlu dikuatkuasakan untuk melindungi maklumat yang diakses, diproses atau disimpan semasa kerja dijalankan di lokasi telekerja. Capaian jarak jauh yang dibenarkan merangkumi: a. Akses daripada sistem rangkaian dalaman. b. Akses daripada sistem rangkaian luaran untuk tujuan telekomunikasi dari lokasi luar pejabat. Pengguna KPN/Agensi boleh diberikan capaian berdasarkan keperluan kerja masing-masing bagi memastikan kerahsiaan dan integriti maklumat yang dihantar melalui rangkaian terpelihara. Penghantaran maklumat melalui capaian jarak jauh **mesti menggunakan kaedah enkripsi** yang selamat dan diluluskan. Lokasi fizikal yang digunakan untuk mengakses sistem ICT KPN/Agensi hendaklah dipastikan selamat dan bebas daripada risiko keselamatan. Penggunaan perkhidmatan capaian jarak jauh hendaklah: a. Mendapat kebenaran terlebih dahulu daripada Pengurus ICT. b. Hanya digunakan oleh pengguna yang telah diberikan kebenaran, dan bertanggungjawab sepenuhnya terhadap penggunaan kemudahan tersebut. Penggunaan perkhidmatan capaian seperti **SSL VPN** hanya dibenarkan selepas mendapat kelulusan Pengurus ICT, dan	Pengurus ICT dan Pengguna

ID	PENERANGAN	PERANAN
	hendaklah mengikut **tahap hak akses serta ID pengguna yang telah diluluskan**.	

6.8 Pelaporan Insiden Keselamatan Maklumat

ID	PENERANGAN	PERANAN
6.8.1	KPN/Agensi hendaklah menyediakan mekanisme yang sesuai bagi membolehkan pengguna melaporkan sebarang insiden keselamatan maklumat yang diperhatikan atau disyaki, melalui saluran pelaporan yang ditetapkan dan dalam tempoh masa yang bersesuaian.	Pengurus ICT, ICTSO, Pentadbir Sistem dan Pengguna
6.8.2	Insiden keselamatan ICT merujuk kepada kejadian yang menjejaskan aset ICT atau situasi yang boleh membawa kepada ancaman keselamatan. Ia juga termasuk sebarang pelanggaran terhadap Polisi Keselamatan Siber (PKS), sama ada secara langsung atau tidak langsung. Semua insiden keselamatan ICT hendaklah dilaporkan dengan segera kepada Pegawai Keselamatan ICT (ICTSO) melalui saluran yang ditetapkan. Pelaporan insiden keselamatan ICT KPN/Agensi seperti mana Prosedur pelaporan insiden keselamatan ICT berdasarkan Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam. Antara contoh insiden keselamatan ICT yang perlu dilaporkan adalah seperti berikut: a. Peralatan/ maklumat hilang atau didedahkan kepada pihak yang tidak dibenarkan, atau disyaki berlaku kehilangan atau pendedahan tersebut.	Pengurus ICT, ICTSO, Pentadbir Sistem dan Pengguna

ID	PENERANGAN	PERANAN
	b. Penggunaan sistem tanpa kebenaran, atau disyaki digunakan tanpa kebenaran. c. Kata laluan atau kawalan akses hilang, dicuri atau didedahkan, atau disyaki berlaku perkara tersebut. d. Kejadian luar biasa pada sistem, seperti fail hilang, sistem gagal berfungsi berulang kali, atau komunikasi tersalah hantar. e. Percubaan menceroboh, penipuan atau kejadian yang tidak dijangka yang boleh menjejaskan keselamatan sistem dan maklumat.	

7 KAWALAN FIZIKAL

7.1 Perimeter Keselamatan Fizikal *(Physical Security Perimeter)*

ID	PENERANGAN	PERANAN
7.1.1	Perimeter keselamatan fizikal bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal, serta kerosakan ke atas premis dan aset ICT milik KPN/Agensi. Ia merangkumi pelaksanaan langkah-langkah keselamatan fizikal bagi melindungi aset, pengguna dan persekitaran daripada ancaman, bahaya atau kerosakan yang mungkin berlaku. Kawalan keselamatan ini melibatkan perlindungan terhadap ruang fizikal seperti bangunan, bilik Server, infrastruktur kritikal dan kawasan-kawasan yang diklasifikasikan sebagai terperingkat.Langkah-langkah yang perlu diambil termasuk yang berikut: a. Menggunakan kawalan perimeter keselamatan seperti pagar, dinding, kawalan akses dan pengawal keselamatan untuk melindungi kawasan yang mengandungi kemudahan pemprosesan maklumat dan maklumat terperingkat. b. Melindungi kawasan terperingkat dengan kawalan masuk yang bersesuaian, bagi memastikan hanya individu yang diberi kebenaran sahaja dibenarkan memasuki kawasan tersebut. c. Reka bentuk dan pelaksanaan keselamatan fizikal di dalam pejabat, bilik dan kemudahan ICT bagi mengurangkan risiko pencerobohan atau kehilangan aset.	Pegawai Keselamatan KPN/Agensi, BKP/BKPSM

ID	PENERANGAN	PERANAN
	d. Penyediaan perlindungan fizikal terhadap bencana seperti kebakaran, banjir, letupan, ancaman manusia serta bencana alam lain yang berpotensi menjejaskan keselamatan aset ICT. e. Melaksanakan perlindungan fizikal dan menyediakan peraturan keselamatan kepada pengguna/pihak ketiga yang bekerja di kawasan terperingkat bagi memastikan pematuhan terhadap langkah keselamatan. f. Mengawal kawasan penghantaran, pemunggahan dan tempat penyimpanan bagi mengelakkan akses oleh pihak yang tidak diberi kebenaran. g. Memasang sistem pemantauan dan pengesanan, seperti kamera litar tertutup (CCTV) atau alat penggera pencerobohan bagi tujuan pengawasan dan tindak balas awal. h. Mendapatkan khidmat nasihat Ketua Pengarah Keselamatan Kerajaan bagi semua cadangan pembinaan, pengubahsuaian, penyewaan, pembangunan atau penaiktarafan fasiliti, selaras dengan keperluan **Arahan Keselamatan (Semakan dan Pindaan 2017)**.	

7.2 Kemasukan Fizikal *(Physical Entry)*

ID	PENERANGAN	PERANAN
7.2.1	**Kawalan Kemasukan Fizikal *(Physical Entry Control)*** Kawalan kemasukan fizikal bertujuan untuk mengawal dan memantau pergerakan keluar masuk individu ke dalam premis bagi menjamin keselamatan aset, maklumat dan kemudahan ICT. Perkara-perkara berikut hendaklah dipatuhi: a. Warga KPN/Agensi hendaklah sentiasa memakai pas keselamatan yang sah sepanjang waktu bertugas. Pas keselamatan hendaklah dikembalikan kepada pihak berkuasa keselamatan apabila berlaku pertukaran Agensi, tamat perkhidmatan atau persaraan. b. Pelawat wajib: i. Mendaftar di kaunter keselamatan; ii. Mendapatkan dan mempamerkan pas keselamatan pelawat sepanjang berada di dalam premis; dan iii. Memulangkan pas tersebut selepas lawatan tamat. c. Akses kepada aset ICT hanya dibenarkan kepada pengguna yang telah diberi kebenaran rasmi oleh organisasi. d. Sebarang kehilangan pas keselamatan hendaklah dilaporkan dengan segera kepada pihak berkuasa keselamatan untuk	BKP/BKPSM/ Pegawai Keselamatan, Warga KPN/Agensi dan pihak ketiga yang mempunyai urusan dengan perkhidmatan KPN/Agensi

ID	PENERANGAN	PERANAN
	tindakan lanjut. e. Warga KPN/Agensi yang hadir bertugas di luar waktu pejabat hendaklah: i. Memohon kebenaran kemasukan terlebih dahulu; dan ii. Melaporkan kehadiran di kaunter keselamatan bagi tujuan rekod dan pemantauan.	
	Kawasan Penyerahan dan Pemunggahan *(Delivery and Loading Areas)* KPN / Agensi hendaklah memastikan semua titik kemasukan fizikal seperti kawasan penyerahan, pemunggahan dan kawasan larangan diurus dengan selamat dan terkawal. Kawasan-kawasan ini hendaklah diasingkan sepenuhnya daripada ruang pemprosesan maklumat, bagi mengelakkan sebarang risiko pencerobohan, gangguan atau akses tanpa kebenaran ke atas sistem, maklumat dan aset ICT.	BKP/BKPSM

7.3 Keselamatan Pejabat, Bilik dan Kemudahan *(Securing Offices, Rooms and Facilities)*

ID	PENERANGAN	PERANAN
7.3.1	Langkah-langkah keselamatan fizikal perlu diambil bagi menghalang akses tanpa kebenaran, gangguan fizikal serta kerosakan terhadap pejabat, bilik dan kemudahan yang digunakan untuk pengoperasian ICT. Perkara-perkara berikut hendaklah dipatuhi:	BKP/BKPSM/ Warga KPN/ Agensi

ID	PENERANGAN	PERANAN
	a. Kawasan seperti tempat kerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data hendaklah dilindungi daripada akses oleh individu yang tidak dibenarkan. b. Akses ke kawasan operasi ICT, pejabat dan bilik berkaitan hendaklah terhad kepada individu yang diberi kebenaran sahaja. c. Petunjuk atau penanda lokasi bagi bilik operasi dan kawasan larangan hendaklah mematuhi keperluan Arahan Keselamatan yang berkuat kuasa, bagi memastikan maklumat lokasi sensitif tidak didedahkan secara terbuka.	

7.4 Pemantauan Keselamatan Fizikal *(Physical Security Monitoring)*

ID	PENERANGAN	PERANAN
7.4.1	Premis fizikal hendaklah dipantau secara berterusan menggunakan sistem pengawasan keselamatan bagi mencegah akses tanpa kebenaran dan memastikan keselamatan aset serta kemudahan ICT. Pemantauan boleh dilaksanakan sama ada secara dalaman atau melalui penyedia perkhidmatan pemantauan keselamatan yang dilantik seperti: a. Pengawal keselamatan yang ditugaskan secara fizikal. b. Sistem penggera pencerobohan.	BKP/BKPSM

ID	PENERANGAN	PERANAN
	c. Sistem pemantauan video, seperti kamera litar tertutup (CCTV). d. Perisian pengurusan maklumat keselamatan fizikal. Semua sistem pemantauan keselamatan hendaklah dilindungi daripada capaian tanpa kebenaran, bagi mengelakkan maklumat pengawasan (seperti rakaman video) daripada diakses oleh pihak yang tidak dibenarkan. Perkara yang perlu dipatuhi: a. Memasang CCTV untuk memantau dan merakam aktiviti di kawasan sensitif, sama ada di dalam atau di luar premis KPN/Agensi. b. Melaksanakan ujian berkala, sekurang-kurangnya sekali setahun, ke atas peralatan keselamatan	

7.5 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran (*Protecting Against Physical and Environmental Threats)*

ID	PENERANGAN	PERANAN
7.5.1	KPN/Agensi hendaklah mereka bentuk dan melaksanakan langkah-langkah perlindungan fizikal bagi memastikan keselamatan premis dan aset ICT daripada sebarang ancaman fizikal dan persekitaran. Langkah-langkah perlindungan ini hendaklah meliputi pencegahan dan pengurangan risiko terhadap: a. Kebakaran b. Banjir c. Letupan	BKP/BKPSM, Pentadbir Pusat Data dan pegawai keselamatan KPN/Agensi

ID	PENERANGAN	PERANAN
	d. Gangguan akibat perbuatan manusia (contohnya vandalisme, sabotaj atau pencerobohan); dan e. Bencana alam atau bencana buatan manusia yang boleh menjejaskan operasi serta keselamatan maklumat dan aset ICT.	

7.6 Bekerja di Kawasan Selamat *(Working In Secure Areas)*

ID	PENERANGAN	PERANAN
7.6.1	Kawasan selamat atau kawasan larangan ditakrifkan sebagai kawasan yang dihadkan aksesnya kepada individu tertentu sahaja. Langkah kawalan keselamatan hendaklah dirangka dan dilaksanakan bagi melindungi aset ICT kritikal yang terdapat dalam premis, termasuk Pusat Data/bilik Server dan kemudahan komunikasi. Kawasan ini perlu dilindungi daripada pelbagai bentuk ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran, bencana alam serta gangguan fizikal yang lain. Langkah-langkah kawalan keselamatan yang perlu dilaksanakan adalah seperti berikut: a. Peralatan ICT utama seperti Server *(server),* peralatan rangkaian dan storan hendaklah ditempatkan di lokasi khas seperti pusat data/bilik server atau bilik yang direka dengan ciri keselamatan fizikal yang tinggi, termasuk sistem pengesanan dan	Pentadbir Pusat Data/Bilik Server dan BKP/BKPSM

ID	PENERANGAN	PERANAN
	pencegahan kebakaran. b. Akses ke kawasan ini hendaklah dihadkan kepada pegawai yang diberi kuasa sahaja dan dipantau secara berterusan. c. Sistem pemantauan seperti CCTV atau peralatan pengawasan lain yang sesuai hendaklah digunakan dan diselenggara secara berkala. d. Rekod log akses dan rakaman CCTV hendaklah diperiksa secara berjadual untuk memastikan tiada pelanggaran keselamatan berlaku. e. Maklumat dan butiran pelawat yang memasuki kawasan larangan hendaklah direkodkan secara lengkap dan disimpan untuk rujukan. f. Pelawat mesti ditemani atau diawasi oleh pegawai bertanggungjawab sepanjang masa mereka berada di kawasan tersebut. g. Lokasi premis ICT hendaklah dipilih di kawasan yang tidak berhampiran dengan: i. Kawasan pemunggahan dan penghantaran; ii. Laluan saliran air; dan iii. Laluan awam yang terbuka f. Tingkap dan pintu hendaklah	

ID	PENERANGAN	PERANAN
	diperkukuh dan sentiasa dikunci, terutamanya apabila tidak digunakan. g. Dinding dan siling kawasan terperingkat perlu diperkukuh bagi mengelakkan sebarang bentuk pencerobohan atau akses tidak sah. h. Akses masuk dan keluar hendaklah dihadkan dan dipusatkan kepada laluan-laluan terkawal sahaja.	

7.7 Meja Kosong dan Skrin Kosong *(Clear Desk and Clear Screen)*

ID	PENERANGAN	PERANAN
7.7.1	Polisi Meja Kosong dan Skrin Kosong adalah satu garis panduan yang digunakan untuk melindungi maklumat sensitif dan menjamin privasi pengguna serta keberkesanan pengurusan keselamatan maklumat di tempat kerja. Polisi ini menekankan supaya tiada maklumat atau bahan sulit ditinggalkan terbuka pada meja kerja atau paparan skrin komputer apabila pengguna tidak berada di tempat masing-masing. Tujuan utama polisi ini adalah untuk: a. Memastikan persekitaran kerja kekal bersih dan teratur. b. Melindungi maklumat daripada pendedahan yang tidak disengajakan. c. Mengurangkan risiko kebocoran maklumat secara fizikal atau	Warga KPN/Agensi, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi.

ID	PENERANGAN	PERANAN
	elektronik. Langkah-langkah yang perlu dipatuhi: a. Aktifkan fungsi kata laluan pada skrin komputer *(password screensaver)* atau log keluar apabila meninggalkan tempat kerja. b. Gunakan fungsi *"Sleep Mode"* atau "*Lock Screen"* apabila komputer tidak digunakan untuk tempoh tertentu. c. Simpan dokumen atau bahan sensitif di dalam laci berkunci atau kabinet fail yang selamat apabila tidak digunakan. d. Ambil semua dokumen yang dicetak, diimbas, difaks atau difotokopi dengan segera bagi mengelakkan pendedahan maklumat. e. Kawal penghantaran dan penerimaan e-mel, khususnya yang mengandungi maklumat sensitif atau terperingkat. f. Hadkan penggunaan mesin fotokopi, pengimbas, kamera digital dan peralatan seumpamanya tanpa kebenaran yang sah. g. Tetapkan peraturan dan panduan berkaitan konfigurasi skrin, seperti:	

ID	PENERANGAN	PERANAN
	i. Menyahaktifkan paparan mesej *pop-up* (contohnya e-mel atau mesej segera) semasa sesi pembentangan, perkongsian skrin, atau ketika bekerja di kawasan awam. ii. Padamkan sebarang maklumat sensitif yang ditulis di papan putih, paparan kaca, atau mana-mana permukaan terbuka selepas digunakan.	
7.7.2	**Peralatan Pengguna Tanpa Kawalan *(Unattended User Equipment)*** Pengguna hendaklah memastikan semua peralatan ICT yang ditinggalkan tanpa pengawasan dilindungi dengan langkah keselamatan yang sewajarnya, bagi mengelakkan akses tanpa kebenaran serta kebocoran maklumat. Peralatan seperti komputer meja, komputer riba, dan terminal hendaklah dikendalikan dengan mematuhi perkara-perkara berikut: a. Menamatkan semua sesi aktif setelah selesai menggunakan sistem atau aplikasi. b. Log keluar *(log-off)* daripada komputer meja, komputer riba, atau Server selepas tamat tugas. c. Memastikan peralatan ICT dilindungi daripada akses oleh individu yang tidak dibenarkan,	Pengguna dan Pihak Ketiga

ID	PENERANGAN	PERANAN
	sama ada dengan mengunci skrin, menyimpan peralatan dengan selamat, atau menggunakan mekanisme kawalan akses yang sesuai.	

7.8 Penempatan dan Perlindungan Peralatan ICT *(Equipment Siting and Protection)*

ID	PENERANGAN	PERANAN
7.8.1	Peralatan ICT hendaklah ditempatkan dan dilindungi dengan sewajarnya bagi mengurangkan risiko terhadap ancaman keselamatan, bahaya persekitaran dan akses tanpa kebenaran. Perlindungan ini termasuk kawalan terhadap lokasi fizikal, penggunaan, serta pengurusan perkakasan dan perisian. Langkah-langkah keselamatan yang perlu dipatuhi: a. **Penggunaan dan Kawalan Akses** i. Kata laluan *(password)* wajib digunakan untuk mengakses sistem komputer. ii. Pengguna tidak dibenarkan menukar kata laluan pentadbir *(administrator)* yang telah ditetapkan oleh pihak ICT. iii. Pengguna bertanggungjawab sepenuhnya terhadap komputer dan akaun yang digunakan.	Pengguna dan pihak ketiga

ID	PENERANGAN	PERANAN
	iv. Log masuk komputer perlu dilindungi, dan hanya pengguna yang dibenarkan sahaja boleh mengaksesnya. b. **Kawalan ke atas Perkakasan** i. Sebarang pertukaran, penambahan atau penggantian perkakasan ICT tanpa kebenaran adalah dilarang sama sekali. ii. Pengguna tidak dibenarkan mengubah kedudukan peralatan ICT dari lokasi asal tanpa kebenaran Pegawai Aset ICT. iii. Peralatan rangkaian seperti suis, penghala, hab dan seumpamanya hendaklah ditempatkan di dalam rak khas yang berkunci. iv. Semua peralatan ICT perlu diletakkan di kawasan yang bersih, teratur dan selamat, termasuklah lokasi berhawa dingin serta mempunyai pengudaraan yang mencukupi. v. Peralatan kritikal hendaklah disokong oleh sistem kuasa sokongan seperti *Uninterruptable Power Supply* (UPS) dan *Generator Set* (Genset). c. **Kawalan ke atas Perisian**	

ID	PENERANGAN	PERANAN
	i. Pengguna dilarang memasang perisian tambahan tanpa kebenaran Pentadbir Sistem. ii. Perisian antivirus di komputer persendirian (bukan aset KPN/Agensi) mesti sentiasa diaktifkan dan dikemas kini, termasuk imbasan ke atas semua media storan sebelum digunakan. iii. Konfigurasi alamat IP tidak boleh diubah daripada tetapan asal tanpa kelulusan Pentadbir Sistem. d. **Pengurusan Aset dan Tanggungjawab Pengguna** i. Peralatan ICT yang ingin dibawa keluar dari premis hendaklah mendapat kelulusan Pegawai Aset ICT dan direkodkan untuk pemantauan. ii. Kehilangan peralatan di luar waktu pejabat hendaklah dilaporkan dan dikendalikan mengikut prosedur pelaporan insiden. iii. Sebarang kerosakan perkakasan ICT perlu dilaporkan segera kepada Pentadbir Sistem untuk tindakan pembaikan.	

ID	PENERANGAN	PERANAN
	iv. Pengguna tidak dibenarkan meletakkan pelekat atau hiasan tidak rasmi pada perkakasan ICT yang boleh merosakkan rupa fizikalnya. v. Setiap pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat yang berada di bawah kawalannya, dan penggunaannya hendaklah terhad kepada urusan rasmi sahaja.	

7.9 Keselamatan Aset di Luar Premis *(Security of Assets Off-Premises)*

ID	PENERANGAN	PERANAN
7.9.1	Aset ICT yang digunakan di luar premis KPN/Agensi adalah lebih terdedah kepada pelbagai risiko keselamatan seperti kehilangan, kecurian, kerosakan fizikal dan pencerobohan maklumat. Oleh itu, langkah perlindungan yang sewajarnya hendaklah diambil untuk memastikan keselamatan peralatan dan maklumat yang dibawa keluar. Perkara yang perlu dipatuhi: a. Peralatan ICT hendaklah sentiasa dikawal dan dilindungi sepanjang masa ketika berada di luar premis. b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri	Pengguna dan Pihak Ketiga

ID	PENERANGAN	PERANAN
	keselamatan yang bersesuaian. c. Tanggungjawab ke atas keselamatan peralatan yang dibawa keluar terletak sepenuhnya di bawah kawalan dan pemantauan pegawai yang menggunakan atau membawa peralatan tersebut.	

7.10 Media Storan *(Storage Media)*

ID	PENERANGAN	PERANAN
7.10.1	**Pengurusan Media Boleh Alih *(Management of Removal Media)*** Media boleh alih merangkumi semua peranti storan mudah alih seperti pemacu USB, cakera keras luaran, cakera padat (CD/DVD), kad memori dan peranti storan mudah alih lain yang digunakan untuk menyimpan, memindahkan atau mengedarkan data. Untuk mengelakkan kerosakan aset, kebocoran maklumat dan gangguan terhadap operasi perkhidmatan, media boleh alih hendaklah dikawal dan dilindungi secara fizikal serta dikendalikan mengikut tahap klasifikasi maklumat. Pemacu atau peranti media boleh alih hanya boleh digunakan jika terdapat keperluan yang sah dan mendapat kelulusan yang sewajarnya. Prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti atau	Pentadbir Sistem dan Pengguna

ID	PENERANGAN	PERANAN
	klasifikasi maklumat. b. Mengehadkan akses kepada media hanya kepada pengguna yang diberi kebenaran, berdasarkan peranan dan keperluan tugas. c. Mengehadkan pengedaran data atau media hanya untuk tujuan rasmi yang diluluskan dan mengikut prosedur yang ditetapkan d. Mengawal dan merekod semua aktiviti penyelenggaraan media bagi mengelakkan kerosakan, kehilangan data atau pendedahan maklumat kepada pihak yang tidak dibenarkan. e. Menyimpan semua jenis media di lokasi yang selamat, terkawal dan berkunci, serta mengelakkan daripada pendedahan kepada suhu, kelembapan atau faktor persekitaran yang boleh menjejaskan kandungannya.	
7.10.2	**Pelupusan Media *(Disposal of Media)*** Pelupusan media ICT hendaklah dilaksanakan secara teratur bagi mengelakkan kebocoran maklumat, penyalahgunaan data dan pendedahan yang tidak dibenarkan. Pelupusan media perlu mendapatkan kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh kerajaan. Media yang mengandungi maklumat terperingkat	Pentadbir Sistem dan Jawatankuasa yang dilantik untuk pelupusan aset.

ID	PENERANGAN	PERANAN
	hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	
7.10.3	**Pengalihan Aset *(Removal of Assets)*** Sebarang pengalihan aset ICT, termasuk peralatan, perisian atau maklumat, dari lokasi asalnya hendaklah dikawal dengan ketat bagi mengelakkan risiko kehilangan, salah guna atau pendedahan maklumat yang tidak dibenarkan. Garis panduan yang perlu dipatuhi adalah seperti berikut: a. Sebarang peralatan ICT yang hendak dibawa keluar dari premis bagi tujuan rasmi hendaklah: i. Mendapat kelulusan Pegawai Aset ICT. ii. Direkodkan secara rasmi bagi tujuan pemantauan dan pengesanan; dan iii. Digunakan hanya bagi tujuan yang dibenarkan. b. Aktiviti peminjaman dan pemulangan peralatan ICT hendaklah direkodkan oleh pegawai yang bertanggungjawab, lengkap dengan maklumat pengguna, tarikh, tujuan penggunaan dan status pemulangan.	Pengguna, Pegawai Aset
7.10.4	**Pengendalian Media *(Media Handling)*** Pengendalian media ICT hendaklah dilaksanakan secara terkawal dan berstruktur bagi melindungi aset ICT	Pentadbir Sistem, dan Pengguna

ID	PENERANGAN	PERANAN
	daripada sebarang pendedahan, pengubahsuaian, pemindahan, pemusnahan tanpa kebenaran, serta gangguan terhadap kelangsungan perkhidmatan. Media yang mengandungi maklumat rasmi, sulit atau terperingkat hendaklah dikendalikan mengikut tahap klasifikasi dan prosedur yang ditetapkan bagi memastikan keselamatan, integriti dan kerahsiaan maklumat sentiasa terpelihara.	

7.11 Utiliti Sokongan *(Supporting Utilities)*

ID	PENERANGAN	PERANAN
7.11.1	Peralatan ICT hendaklah dilindungi daripada gangguan operasi yang disebabkan oleh kegagalan bekalan utiliti seperti bekalan kuasa, sistem penyejukan, dan pengudaraan. Gangguan kepada utiliti sokongan boleh menyebabkan kerosakan peralatan, kehilangan data dan menjejaskan kelangsungan perkhidmatan ICT. Garis Panduan: a. Semua peralatan ICT penting hendaklah disokong oleh sistem bekalan kuasa kecemasan seperti: i. *Uninterruptible Power Supply* (UPS); dan	Pentadbir Sistem, BKP/BKPSM dan Pengurusan Fasiliti

ID	PENERANGAN	PERANAN
	ii. Generator Set *(Genset),* khususnya bagi peralatan kritikal seperti Server (server), storan pusat data dan peralatan rangkaian utama. b. Sistem penyejukan dan pengudaraan yang sesuai hendaklah disediakan di bilik server, bilik komunikasi dan ruang ICT bagi mengelakkan pemanasan berlebihan *(overheating).* c. Semua utiliti sokongan termasuk sistem bekalan kuasa, UPS, Gen-Set, penyejukan dan penggera suhu hendaklah: i. Diselenggara secara berkala, sekurang-kurangnya setahun sekali atau mengikut jadual penyelenggaraan yang diluluskan; dan ii. Direkodkan dalam log penyelenggaraan untuk tujuan pemantauan dan audit. d. KPN/Agensi hendaklah memastikan terdapat pelan sokongan dan pemulihan utiliti sekiranya berlaku gangguan bagi memastikan kesinambungan operasi ICT.	

7.12 Keselamatan Kabel *(Cabling Security)*

ID	PENERANGAN	PERANAN
7.12.1	Kabel kuasa dan telekomunikasi yang digunakan untuk menghantar data dan menyokong perkhidmatan ICT perlu dilindungi dengan baik bagi mengelakkan risiko pintasan maklumat, gangguan perkhidmatan atau kerosakan fizikal. Langkah-langkah keselamatan yang perlu dipatuhi: a. Gunakan kabel yang mematuhi spesifikasi teknikal yang telah ditetapkan. b. Pastikan kabel dilindungi daripada kerosakan sama ada akibat tindakan manusia atau keadaan persekitaran seperti air, haba atau gangguan elektrik. c. Laluan pemasangan kabel perlu disusun dengan kemas dan dilindungi sepenuhnya, contohnya: i. Diletakkan di dalam saluran kabel *(trunking/conduit)*; ii. Tidak terdedah di kawasan umum atau mudah dicapai oleh orang awam. d. Elakkan pemasangan kabel secara terbuka bagi mengurangkan risiko pintasan maklumat *(wire tapping)*.	Pentadbir Sistem, BKP/BKPSM dan Pengurusan Fasiliti

ID	PENERANGAN	PERANAN
	e. Setiap kabel perlu dilabel dengan jelas untuk memudahkan kerja-kerja penyelenggaraan dan pemantauan.	

7.13 Penyelenggaraan Peralatan *(Equipment Maintenance)*

ID	PENERANGAN	PERANAN
7.13.1	**kebolehsediaan *(availability)*, kerahsiaan *(confidentiality)*** Peralatan ICT perlu diselenggara secara berkala dan mengikut keperluan bagi memastikan ia sentiasa berada dalam keadaan baik, boleh digunakan serta menjamin aspek kebolehsediaan *(availability)*, kerahsiaan *(confidentiality)* dan integriti *(integrity)* maklumat serta sistem. Langkah-langkah keselamatan yang perlu dipatuhi: a. Setiap peralatan ICT hendaklah diselenggara oleh pegawai yang bertanggungjawab. b. Penyelenggaraan mestilah mengikut spesifikasi oleh pengeluar yang ditetapkan. c. Hanya personel ICT terlatih atau pihak ketiga yang dilantik atau dibenarkan menjalankan kerja penyelenggaraan. d. Semua peralatan hendaklah diperiksa dan diuji sebelum dan selepas penyelenggaraan untuk memastikan ia berfungsi	Pegawai Aset, Pentadbir Sistem, Pengguna dan Pihak Ketiga.

ID	PENERANGAN	PERANAN
	dengan baik dan tidak mengganggu sistem sedia ada. e. Pihak pengguna mesti dimaklumkan lebih awal sebelum sebarang kerja penyelenggaraan dilaksanakan, sama ada mengikut jadual yang dirancang atau bagi keperluan kecemasan.	

7.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan *(Secure Disposal or Re-Use of Equipment)*

ID	PENERANGAN	PERANAN
7.14.1	Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bebas daripada data sensitif dan perisian berlesen sebelum dilupuskan atau digunakan semula. Data tersebut mestilah dikeluarkan sepenuhnya atau ditulis ganti *(overwrite)* menggunakan kaedah yang selamat. Pelupusan mestilah mematuhi prosedur dan dilaksanakan secara terkawal serta menyeluruh, bagi memastikan tiada maklumat yang terlepas daripada kawalan KPN/Agensi. Langkah-langkah berikut hendaklah diambil: a. **Bagi Pemadaman Data Secara Selamat** Bagi peralatan ICT yang akan dilupuskan atau dipindah milik, semua data dalam media storan hendaklah dipadamkan	Pegawai Aset, Pentadbir Sistem dan Pengguna

ID	PENERANGAN	PERANAN
	sepenuhnya menggunakan kaedah pemusnahan data yang selamat dan diiktiraf. b. **Penilaian Peralatan ICT** Pegawai Aset bertanggungjawab menilai dan mengenal pasti sama ada peralatan ICT boleh dilupuskan atau sebaliknya, berdasarkan keadaan fizikal dan fungsinya. c. **Penyimpanan Sebelum Pelupusan** Peralatan yang dikenal pasti untuk dilupuskan hendaklah disimpan di lokasi khas yang mempunyai ciri keselamatan yang mencukupi, bagi mengelakkan sebarang capaian tanpa kebenaran sebelum proses pelupusan dilaksanakan. d. **Proses Pelupusan Secara Berpusat** Semua proses pelupusan peralatan ICT hendaklah dilaksanakan secara berpusat dan mengikut tatacara pelupusan semasa yang ditetapkan oleh kerajaan, termasuk rujukan kepada Pekeliling Perbendaharaan dan garis panduan daripada agensi pusat. e. **Larangan kepada Pengguna ICT:** Pengguna ICT adalah dilarang sama sekali daripada melakukan perkara berikut:	

ID	PENERANGAN	PERANAN
	i. Menyimpan peralatan ICT yang telah dikenal pasti untuk dilupuskan bagi kegunaan peribadi; ii. Mencabut, menanggalkan atau menyimpan komponen dalaman komputer seperti RAM, cakera keras (HDD), *motherboard* dan seumpamanya; iii. Memindahkan atau menyimpan peralatan luaran seperti AVR, pembesar suara *(speaker)* dan lain-lain ke lokasi lain tanpa kebenaran bertulis; iv. Melupuskan sendiri peralatan ICT tanpa melalui saluran rasmi dan tatacara yang ditetapkan oleh pihak KPN/Agensi . **Tanggungjawab Pengguna:** a. Pengguna ICT bertanggungjawab memastikan semua maklumat sulit dan rahsia yang terdapat dalam komputer disalin terlebih dahulu ke dalam media storan kedua (seperti pemacu USB) sebelum proses penghapusan data dilakukan. b. Data dan maklumat dalam peralatan ICT yang hendak dilupuskan atau dipindah milik hendaklah dihapuskan secara kekal. c. Sekiranya data perlu disimpan	

ID	PENERANGAN	PERANAN
	untuk rujukan masa hadapan, pengguna hendaklah membuat salinan simpanan terlebih dahulu sebelum peralatan dihantar untuk pelupusan. **Maklumat Tambahan dan Rujukan:** Pelupusan aset ICT hendaklah dirujuk kepada: i. Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang sedang berkuat kuasa; ii. Arahan Keselamatan dan garis panduan pelupusan dokumen oleh Arkib Negara Malaysia(ANM) bagi pelupusan dokumen rasmi. **Pegawai Aset bertanggungjawab untuk:** **a.** Merekod butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem pengurusan Aset.	

8 KAWALAN TEKNOLOGI

8.1 Peranti Titik Hujung Pengguna *(User Endpoint Devices)*

ID	PENERANGAN	PERANAN
8.1.1	**Polisi Peranti Endpoint *(Endpoint Device Policy)*** Polisi ini bertujuan untuk menetapkan kawalan dan langkah-langkah keselamatan yang perlu dilaksanakan bagi mengurus risiko yang timbul melalui penggunaan peranti *endpoint* (peranti titik hujung) seperti komputer riba, tablet, telefon pintar dan peranti storan mudah alih dalam mengakses, memproses atau menyimpan maklumat rasmi organisasi.	Pentadbir Sistem, Pentadbir Rangkaian ICT dan Pengguna
8.1.2	Sokongan teknikal bertanggungjawab mengurus dan menyebarkan dasar serta langkah-langkah keselamatan berkaitan penggunaan peranti *endpoint*, termasuk perkara-perkara berikut: a. **Pengelasan Maklumat dan Pengendalian Peranti** Menentukan jenis maklumat dan tahap klasifikasi yang boleh diakses, diproses atau disimpan oleh peranti *endpoint*. b. **Sambungan Rangkaian** Menetapkan peraturan berkaitan sambungan peranti ke rangkaian dalaman, rangkaian awam dan perkhidmatan luar pejabat. c. **Keselamatan Storan dan Pemindahan Data** Menjalankan penyulitan (enkripsi) ke atas peranti storan mudah alih yang mengandungi	Pentadbir Server, Pentadbir Rangkaian, Sokongan Teknikal (*Technical Support)*

ID	PENERANGAN	PERANAN
	data terperingkat. d. **Perlindungan Terhadap Perisian Hasad** Memastikan semua peranti *endpoint* dilengkapi dan dikemaskini dengan perisian antivirus serta perisian keselamatan yang sah.	
	Semua pengguna peranti *endpoint* bertanggungjawab memastikan pematuhan kepada perkara-perkara berikut: a. **Perlindungan Fizikal** Memastikan peranti dijaga rapi dan dilindungi daripada kehilangan, kecurian atau kerosakan. b. **Kawalan Perisian** i. Tidak dibenarkan memasang sebarang perisian tanpa kebenaran; ii. Memastikan perisian yang digunakan sentiasa dikemaskini dengan versi dan patch terkini. c. **Kawalan Akses** i. Menggunakan peranti hanya untuk tujuan rasmi yang dibenarkan; ii. Kawalan ke atas capaian ke sistem maklumat dan perkhidmatan dalam talian mengikut keperluan tugas. d. **Penggunaan Teknik Kriptografi**	Warga KPN/Agensi

ID	PENERANGAN	PERANAN
	Menggunakan kawalan akses dan teknik kriptografi yang ditetapkan oleh unit ICT bagi memastikan keselamatan data terperingkat. e. **Penyimpanan Selamat** Peranti hendaklah disimpan di tempat yang selamat apabila tidak digunakan bagi mengelakkan capaian tidak dibenarkan.	
8.1.2	**Peralatan Pengguna Tanpa Kawalan *(Unattended User Equipment)*** Pengguna hendaklah memastikan bahawa semua peralatan ICT yang ditinggalkan tanpa pengawasan mempunyai langkah perlindungan yang sewajarnya bagi mengelakkan sebarang akses yang tidak dibenarkan atau pencerobohan keselamatan. Bagi tujuan tersebut, pengguna adalah bertanggungjawab untuk mematuhi perkara berikut: a. Menamatkan sesi aktif *(active session)* selepas selesai menjalankan tugasan; b. Melaksanakan log keluar *(log-off)* bagi peranti dan Server selepas waktu bekerja atau apabila tidak digunakan; c. Memastikan peranti sentiasa dilindungi dan tidak boleh diakses oleh individu yang tidak diberi kuasa.	Warga KPN/Agensi/ Pihak Ketiga

ID	PENERANGAN	PERANAN
8.1.3	**Perlindungan Maklumat pada Peranti Pengguna** Pengguna adalah bertanggungjawab untuk melindungi sebarang maklumat yang disimpan pada peranti ICT masing-masing daripada sebarang bentuk pencerobohan, kehilangan, atau capaian tanpa kebenaran. Bagi memastikan keselamatan maklumat, pengguna hendaklah mengambil langkah-langkah berikut: a. **Menggunakan Kata Laluan yang Kukuh** Pengguna hendaklah menetapkan kata laluan yang kukuh dan sukar diteka. Kata laluan tersebut hendaklah mengandungi gabungan huruf besar, huruf kecil, nombor dan simbol khas. Kata laluan tidak boleh dikongsi dan perlu ditukar secara berkala. b. **Menggunakan Perisian Antivirus yang Dikemaskini** Perisian antivirus hendaklah dipasang dan dikemaskini secara berkala untuk melindungi peranti pengguna daripada ancaman virus, perisian hasad *(malware)*, dan pencerobohan siber. c. **Mengemaskini Sistem Operasi dan Perisian** Sistem operasi dan perisian aplikasi hendaklah dikemaskini secara berkala bagi memastikan perlindungan terhadap kelemahan *(vulnerabilities)* terkini yang	Warga KPN/Agensi

ID	PENERANGAN	PERANAN
	boleh dieksploitasi oleh pihak tidak bertanggungjawab.	

8.2 Pengurusan Hak Akses Istimewa *(Management of Privileged Access Rights)*

ID	PENERANGAN	PERANAN
8.2.1	Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan, dikawal serta diselia dengan teliti bagi mengelakkan penyalahgunaan dan memastikan keselamatan sistem ICT. Hak capaian sistem ICT hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu untuk tempoh ditetapkan berdasarkan peranan berikut: a. Mengenalpasti pengguna yang memerlukan hak akses istimewa untuk setiap sistem atau proses; b. Memberi hak akses istimewa kepada pengguna dengan keperluan minimum untuk peranan fungsian mereka; c. Mengekalkan proses menentukan siapa yang boleh meluluskan hak akses istimewa dan merekod semua keistimewaan yang diperuntukkan; d. Menentukan dan melaksanakan keperluan bagi pengguna yang telah tamat tempoh hak akses istimewa;	Pentadbir Sistem Aplikasi, Pentadbir Pentadbir Sistem, Pembangunan Sistem Aplikasi, Pentadbir Server, Pemilik Sistem, Pengguna dan Pentadbir Sistem ICT

ID	PENERANGAN	PERANAN
	dan e. Menyemak pengguna yang diberi hak akses istimewa secara berkala atau selepas sebarang perubahan jabatan.	

8.3 Sekatan Akses Maklumat *(Information Access Restriction)*

ID	PENERANGAN	PERANAN
8.3.1	Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan dan dikawal. Kawalan ini bertujuan untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat serta sistem, dan hendaklah merangkumi perkara-perkara berikut: a. Melarang capaian oleh pengguna yang tidak berdaftar atau tidak sah terhadap maklumat sensitif atau sistem kritikal. b. Menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan ICT. c. Menghadkan capaian data mengikut keperluan tugas pengguna, termasuk hanya membenarkan akses kepada data yang relevan. d. Mengawal identiti atau kumpulan identiti pengguna yang diberi hak capaian seperti	Pengguna, Pentadbir Sistem Aplikasi, ICTSO, Ketua Agensi/ Ketua Bahagian

ID	PENERANGAN	PERANAN
	baca *(read),* tulis *(write),* padam *(delete),* dan laksana *(execute)* e. Menyediakan kawalan capaian secara fizikal atau logikal bagi mengasingkan aplikasi dan data yang bersifat sensitif daripada sistem atau persekitaran lain.	

8.4 Kawalan Akses Kepada Kod Sumber Program *(Access Control to Source Code)*

ID	PENERANGAN	PERANAN
8.4.1	Capaian kepada kod sumber program hendaklah dihadkan dan dikawal secara ketat bagi mengelakkan sebarang perubahan tanpa kebenaran, kehilangan data, atau penyalahgunaan. Capaian hanya boleh diberikan kepada pegawai yang dibenarkan berdasarkan keperluan tugas serta tertakluk kepada kawalan dan prosedur yang ditetapkan. Perkara-perkara berikut hendaklah diambil kira dalam pengurusan kawalan akses kepada kod sumber: a. **Perekodan Log Akses *(Audit Trail)*** Semua aktiviti capaian terhadap kod sumber hendaklah direkod dan disimpan melalui log audit yang boleh disemak bagi tujuan pengesanan, pemantauan dan penyiasatan insiden.	Pengarah Projek, Pengurus Projek dan Pentadbir Sistem, Pembangun Sistem Aplikasi

ID	PENERANGAN	PERANAN
	b. **Kawalan Perubahan** Sebarang penyelenggaraan, pengubahsuaian, atau penyalinan kod sumber hendaklah dilaksanakan melalui proses kawalan perubahan *(change control)* yang diluluskan, direkod dan dipantau. c. **Hak Milik Kod Sumber** Kod sumber bagi semua sistem aplikasi dan perisian yang dibangunkan untuk kegunaan rasmi hendaklah menjadi hak milik KPN/Agensi dan tidak boleh dipindah milik tanpa kelulusan rasmi. d. **Akses Mengikut Keperluan** i. Akses baca dan/atau tulis hendaklah diberikan berdasarkan prinsip keperluan tugas *(need-to-know)* dan dikawal bagi mengurangkan risiko penyalahgunaan atau pengubahsuaian yang tidak sah. ii. Semua akses hendaklah dikendalikan menurut prosedur keselamatan yang ditetapkan.	

8.5 Prosedur Log Masuk yang Selamat *(Secure Log-on Procedure)*

ID	PENERANGAN	PERANAN
8.5.1	Capaian ke atas aplikasi sistem hendaklah dikawal dengan kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian tanpa kebenaran, selaras dengan keperluan keselamatan maklumat KPN/Agensi. Langkah-langkah kawalan yang perlu dilaksanakan adalah seperti berikut: a. **Pengesahan Pengguna yang Sah** Hanya pengguna yang dibenarkan sahaja boleh mengakses aplikasi sistem, dan pengesahan identiti hendaklah dilaksanakan mengikut peraturan dan dasar KPN/Agensi . b. **Penjanaan Amaran Keselamatan** Sistem hendaklah mampu menjana amaran *(alert)* sekiranya berlaku percubaan log masuk yang mencurigakan atau pelanggaran polisi semasa proses log masuk. c. **Pengawalan Capaian Berdasarkan Prosedur** Capaian terhadap aplikasi sistem hendaklah dikawal secara berstruktur dan berpandukan kepada prosedur yang diluluskan, termasuk mengikut peranan dan tanggungjawab pengguna	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	(role-based access control). d. **Pengurusan Kata Laluan secara Interaktif** Sistem hendaklah menyediakan mekanisme pengurusan kata laluan yang mesra pengguna dan menggalakkan penggunaan kata laluan yang kukuh. e. **Jejak Aud*it (Audit Trail)*** Semua aktiviti capaian terhadap aplikasi sistem hendaklah direkodkan melalui log audit yang boleh disemak, bagi tujuan pemantauan, pengesanan insiden dan penyiasatan.	
8.5.2	**Sistem Pengurusan Kata Laluan *(Password Management System)*** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KPN/Agensi seperti yang berikut: a. **Kerahsiaan Kata Laluan** Kata laluan adalah bersifat rahsia dan tidak boleh dikongsi, didedahkan atau dimaklumkan kepada mana-mana individu dalam apa jua keadaan dan sebab. b. **Penukaran Kata Laluan Sekiranya Disyaki Kompromi** Pengguna hendaklah menukar kata laluan dengan serta-merta sekiranya terdapat sebarang petunjuk atau syak wasangka bahawa kata laluan telah terdedah atau dikompromi.	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	c. **Panjang dan Kerumitan Kata Laluan** Kata laluan hendaklah mempunyai sekurang-kurangnya **DUA BELAS (12) AKSARA**, dan mengandungi gabungan huruf besar, huruf kecil, nombor dan aksara khas *(alphanumeric + special characters*) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad. d. **Kitar Semula Kata Laluan** Tiga (3) kata laluan terakhir yang pernah digunakan tidak boleh digunakan semula. e. **Kata Laluan Tidak Boleh Dicatat atau Disimpan** Kata laluan hendaklah diingati dan tidak boleh dicatat, disimpan dalam media fizikal atau digital, atau dikongsi melalui sebarang medium. f. **Pengaktifan Kata Laluan Paparan Kunci *(Lock Screen)*** Kata laluan bagi paparan kunci *(lock screen)* hendaklah diaktifkan, khususnya pada komputer atau peranti yang terletak di kawasan gunasama atau awam. g. **Kata Laluan Tidak Dipaparkan** Kata laluan hendaklah tidak dipaparkan secara visual semasa input (contoh: asterisk	

ID	PENERANGAN	PERANAN
	atau dot), tidak dilaporkan dalam sistem, dan tidak disimpan dalam kod sumber atau fail konfigurasi. h. **Penguatkuasaan Penukaran Kata Laluan** Pengguna hendaklah dipaksa menukar kata laluan: i. pada kali pertama log masuk, ii. selepas penetapan semula kata laluan *(password reset),* atau iii. apabila ditetapkan oleh pentadbir sistem. i. **Kata Laluan Tidak Sama dengan ID Pengguna** Kata laluan tidak boleh sama dengan nama pengguna atau pengenalan identiti *(User* ID*).* j. **Had Percubaan Log Masuk** Percubaan log masuk yang menggunakan kata laluan salah dihadkan kepada maksimum tiga (3) kali sahaja. Selepas had dicapai, capaian ke sistem akan disekat secara automatik, dan hanya boleh diaktifkan semula oleh pentadbir sistem. k. **Kemudahan Menukar Kata Laluan** Sistem yang digunakan atau dibangunkan hendaklah menyediakan kemudahan penukaran kata laluan secara kendiri *(self-service)* oleh pengguna.	

8.6 Pengurusan Kapasiti *(Capacity Management)*

ID	PENERANGAN	PERANAN
8.6.1	Penggunaan sumber ICT hendaklah dipantau secara berterusan, disesuaikan mengikut keperluan semasa, dan unjuran kapasiti hendaklah disediakan bagi memenuhi keperluan jangka masa hadapan. Langkah ini bertujuan untuk memastikan prestasi sistem yang optimum dan berterusan dapat dicapai serta menyokong pertumbuhan sistem ICT KPN/Agensi secara berkesan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. **Perancangan dan Kawalan Kapasiti ICT** Kapasiti setiap komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal secara teliti oleh pegawai yang bertanggungjawab bagi memastikan keupayaannya mencukupi, bersesuaian serta menyokong pembangunan dan operasi sistem ICT pada masa hadapan. b. **Pengambilan Kira Aspek Keselamatan Siber** Unjuran kapasiti hendaklah merangkumi ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan perkhidmatan *(service disruption)*, kelewatan sistem, atau kerugian akibat perubahan yang tidak dirancang dan tidak selamat.	Pemilik Sistem, Pentadbir Sistem, Pentadbir Server dan Pentadbir Pangkalan Data

8.7 Perlindungan daripada Perisian Hasad *(Protection Against Malware)*

ID	PENERANGAN	PERANAN
8.7.1	Bagi melindungi aset ICT KPN/Agensi daripada ancaman perisian hasad *(malware)*, kawalan pengesanan, pencegahan dan pemulihan hendaklah dilaksanakan secara menyeluruh serta digabungkan dengan peningkatan kesedaran pengguna terhadap ancaman dan kaedah serangan. Langkah-langkah kawalan yang perlu dilaksanakan termasuk: a. **Pemasangan dan Penggunaan Sistem Keselamatan** Menggunakan perisian dan sistem keselamatan seperti antivirus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) dengan konfigurasi yang betul dan selamat mengikut prosedur penggunaan yang diluluskan. b. **Penggunaan Perisian Tulen** Memastikan semua perisian yang dipasang adalah tulen, berdaftar dan dilindungi di bawah undang-undang yang berkuatkuasa. Penggunaan perisian cetak rompak adalah dilarang sama sekali. c. **Imbasan Antivirus** Menjalankan imbasan antivirus terhadap semua perisian dan sistem sebelum digunakan atau dipasang ke dalam persekitaran ICT organisasi.	Pentadbir Sistem, Pengguna, Pentadbir Server dan Pentadbir Pangkalan Data

ID	PENERANGAN	PERANAN
	d. **Kemas Kini Terkini** Memastikan perisian antivirus dikemaskini secara berkala dengan *signature/pattern* terkini bagi membolehkan pengesanan perisian hasad baharu. e. **Pemantauan Berkala** Menyemak dan memantau sistem serta kandungan maklumat secara berkala bagi mengesan sebarang aktiviti mencurigakan termasuk kehilangan atau kerosakan data. f. **Program Kesedaran Pengguna** Pengguna hendaklah menyertai program kesedaran keselamatan siber yang merangkumi topik berkaitan perisian hasad, kaedah penyebaran serta cara mencegah dan menanganinya. g. **Peruntukan dalam Kontrak Pembekalan Perisian** Menyertakan klausa tanggungan dalam kontrak pembekalan perisian, yang membolehkan tuntutan pembaikan dibuat sekiranya perisian yang dibekalkan mengandungi unsur perisian hasad. h. **Pelan Pemulihan dan Kesinambungan Perkhidmatan**	

ID	PENERANGAN	PERANAN
	Menyediakan dan menguji pelan kesinambungan perkhidmatan (BCP/DRP) bagi membolehkan pemulihan segera sekiranya berlaku serangan perisian hasad. i. **Penetapan Tanggungjawab dan Prosedur Perlindungan** Menetapkan dengan jelas prosedur dan tanggungjawab bagi perlindungan terhadap perisian hasad termasuk pengesanan, respons dan pemulihan. j. **Pemantauan Ancaman Baharu:** Melaksanakan prosedur pemantauan berkala bagi mendapatkan maklumat terkini berkaitan perisian hasad baharu daripada sumber yang dipercayai. k. **Pengesahan Sumber Maklumat** Memastikan maklumat berkaitan ancaman perisian hasad yang diterima adalah daripada sumber yang sah dan disahkan, sebelum dijadikan rujukan atau digunakan dalam sebarang tindakan mitigasi.	

8.8 Pengurusan Kerentanan Teknikal *(Management of Technical Vulnerabilities)*

ID	PENERANGAN	PERANAN
8.8.1	Maklumat berkaitan kerentanan teknikal dalam sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat. KPN/Agensi perlu menilai tahap keterdedahan kepada kerentanan tersebut dan mengambil tindakan yang bersesuaian bagi mengurangkan risiko keselamatan yang mungkin berlaku. Langkah kawalan terhadap kerentanan teknikal perlu dilaksanakan bagi melindungi sistem maklumat, perisian dan infrastruktur teknologi daripada ancaman serta serangan yang boleh mengeksploitasi kelemahan yang wujud. Perkara-perkara berikut hendaklah dipatuhi bagi memastikan pengurusan kerentanan teknikal dilaksanakan secara berkesan: a. **Melaksanakan Ujian Penembusan *(Penetration Testing)*** Menjalankan ujian penembusan *(penetration testing)* secara berkala ke atas sistem aplikasi dan sistem operasi untuk mengenal pasti kerentanan yang wujud. b. **Mengenal Pasti dan Menilai Risiko Kerentanan** Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan dalam sistem, perisian dan rangkaian di	Pentadbir Sistem, CSIRT KPN/Agensi, Pentadbir Server dan Pentadbir Pangkalan Data

ID	PENERANGAN	PERANAN
	peringkat KPN/Agensi . c. **Melaksanakan Tindakan Pembetulan dan Penambahbaikan** Mengambil tindakan pembetulan ke atas kerentanan yang dikenal pasti, termasuk penambahbaikan kawalan keselamatan dan konfigurasi sistem. d. **Pemantauan Berterusan** Memantau sistem dan perisian secara berterusan bagi mengesan kerentanan baharu yang mungkin timbul. e. **Mengamalkan Keselamatan Teknikal yang Terbaik** Melaksanakan dan memastikan pematuhan terhadap amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan, selaras dengan piawaian serta garis panduan keselamatan siber yang berkuat kuasa.	

8.9 Pengurusan konfigurasi *(Configuration Management)*

ID	PENERANGAN	PERANAN
8.9.1	Pengurusan konfigurasi bertujuan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi mengikut tetapan keselamatan yang ditetapkan serta mengelakkan sebarang perubahan tidak sah oleh pihak yang tidak dibenarkan. Ia merupakan elemen penting dalam memastikan kestabilan	Pentadbir Sistem, Pentadbir Server, Pentadbir Rangkaian

ID	PENERANGAN	PERANAN
	operasi dan keselamatan sistem ICT organisasi. Bagi memastikan kawalan konfigurasi dilaksanakan dengan berkesan, perkara-perkara berikut hendaklah dipatuhi: a. **Tadbir Urus Konfigurasi** Menetapkan tadbir urus yang memantau, meluluskan dan merekodkan sebarang perubahan konfigurasi sebelum ia dilaksanakan. b. **Prosedur Pengurusan Konfigurasi** Menyediakan prosedur rasmi bagi pelaksanaan, pemantauan dan semakan semula konfigurasi yang melibatkan perkakasan, perisian, perkhidmatan dan rangkaian. c. **Penyimpanan Konfigurasi yang Selamat** Menyimpan konfigurasi mengikut prosedur atau arahan semasa, selaras dengan nilai dan klasifikasi maklumat, serta mengambil kira keperluan dan sensitiviti operasi KPN/Agensi . d. **Perlindungan Akses kepada Fail Konfigurasi** Mengawal akses kepada fail konfigurasi dengan mekanisme kawalan yang ditetapkan, bagi mengelakkan sebarang capaian atau perubahan yang tidak dibenarkan. e. **Pemantauan dan Pengesahan Konfigurasi**	

ID	PENERANGAN	PERANAN
	Memantau konfigurasi secara berterusan bagi mengesahkan tetapan konfigurasi dan menilai keberkesanan kawalan keselamatan yang dilaksanakan.	

8.10 Penghapusan/Pelupusan/ Sanitasi Maklumat *(Information Deletion)*

ID	PENERANGAN	PERANAN
8.10.1	Penghapusan, pelupusan atau sanitasi maklumat bertujuan untuk mengelakkan pendedahan maklumat sensitif serta memastikan pematuhan terhadap keperluan undang-undang, statutori, peraturan dan kontrak berkaitan pelupusan maklumat. Semua maklumat rasmi dan rahsia rasmi kerajaan yang disimpan dalam Server, cakera keras, rangkaian, peranti USB atau sebarang media storan lain hendaklah dilupuskan mengikut ketetapan yang dinyatakan dalam Surat Pekeliling Am Bilangan 4 Tahun 2022 (SPA 4/2022): Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam, atau peraturan lain yang sedang berkuat kuasa. Perkara-perkara berikut hendaklah dipatuhi: a. **Menentukan Kaedah Penghapusan Maklumat yang Sesuai** Menetapkan kaedah penghapusan atau sanitasi maklumat yang bersesuaian mengikut keperluan dan sensitiviti maklumat serta	Semua

ID	PENERANGAN	PERANAN
	selaras dengan dasar KPN/Agensi. b. **Merekod Proses Penghapusan** Merekod setiap proses penghapusan sebagai bukti bahawa maklumat telah dilupuskan dengan betul dan mengikut prosedur. c. **Mendapatkan Bukti Penghapusan oleh Pihak Ketiga** Sekiranya perkhidmatan pelupusan dikendalikan oleh pembekal luar, bukti penghapusan atau sanitasi maklumat hendaklah diperoleh daripada pihak tersebut sebagai pengesahan.	

8.11 Penyamaran Data *(Data Masking)*

ID	PENERANGAN	PERANAN
8.11.1	Penyamaran data dilaksanakan bagi melindungi data sensitif seperti Maklumat Boleh Mengenal Pasti Individu *(Personal Identifiable Information* – PII) dan data terperingkat, dengan mengambil kira keperluan perkhidmatan, dasar kawalan capaian serta dasar-dasar lain yang berkaitan, tertakluk kepada keperluan perundangan dan peraturan yang berkuatkuasa. Bagi mengelakkan pendedahan data peribadi dan data terperingkat kepada pihak yang tidak dibenarkan, penyamaran data perlu dilaksanakan sebagai salah satu langkah kawalan keselamatan untuk	Pentadbir Sistem/Pengurus Rekod KPN/Agensi

ID	PENERANGAN	PERANAN
	melindungi integriti dan reputasi KPN/Agensi. Antara teknik penyamaran data yang boleh digunakan dalam sistem aplikasi atau peralatan termasuklah: a. **Enkripsi** Data disulitkan dan hanya boleh diakses oleh pengguna yang memiliki kunci penyahsulitan *(decryption key)*. b. **Penggantian dengan Nilai Kosong *(Null)* atau Pemadaman Sebahagian Data** Contohnya, membuang sebahagian huruf atau nombor untuk mengelakkan paparan penuh data kepada pengguna yang tidak dibenarkan. c. **Pengubahan Nilai Asal** Mengubah nombor, tarikh atau butiran lain daripada nilai sebenar tanpa menjejaskan fungsi sistem. **d. Penggantian Nilai** Menukar data sensitif kepada nilai lain yang tidak berkaitan tetapi mengekalkan struktur asal data. **e. Penukaran kepada Nilai Ringkasan *(Hash Value)*** Data ditukar kepada bentuk ringkasan kriptografi yang tidak boleh dipulihkan semula kepada nilai asal, bagi memastikan kerahsiaan data.	

8.12 Pencegahan Ketirisan Data *(Data Leakage Prevention)*

ID	PENERANGAN	PERANAN
8.12.1	Pendedahan dan pengeluaran maklumat tanpa kebenaran boleh menjejaskan kerahsiaan, integriti dan reputasi organisasi. Justeru, langkah-langkah pencegahan ketirisan data perlu dilaksanakan bagi mengesan dan menghalang sebarang kebocoran maklumat. Antara langkah yang perlu diambil termasuk: a. **Pengenalpastian dan Pengklasifikasian Maklumat** Mengenal pasti dan mengklasifikasikan maklumat mengikut tahap sensitiviti bagi memastikan perlindungan yang sewajarnya, terutamanya terhadap data peribadi dan data terperingkat. b. **Pemantauan Saluran Kebocoran Data** Memantau punca atau saluran berpotensi yang boleh menyebabkan kebocoran data, seperti emel, peranti storan mudah alih, aplikasi awan *(cloud)*, atau capaian jauh. c. **Sekatan dan Kawalan Capaian Pengguna** Mengehadkan capaian pengguna kepada maklumat berdasarkan keperluan tugasan *(need-to-know basis)* dan tanggungjawab kerja. d. **Perlindungan Proses**	Pentadbir Sistem / Pengurus Rekod KPN/Agensi , Pentadbir Server dan Pentadbir Pangkalan Data

ID	PENERANGAN	PERANAN
	Sandaran Data Memastikan data yang disandarkan dilindungi melalui mekanisme seperti penyulitan *(encryption)*, kawalan akses dan penyimpanan di lokasi yang selamat.	

8.13 Sandaran Maklumat *(Information Backup)*

ID	PENERANGAN	PERANAN
8.13.1	Bagi memastikan keselamatan, kesinambungan operasi serta pemulihan sistem yang berkesan sekiranya berlaku bencana, proses sandaran maklumat, perisian dan imej sistem hendaklah dilaksanakan dan diuji secara berkala mengikut prosedur sandaran yang telah dipersetujui. Sandaran juga perlu dilakukan setiap kali berlaku perubahan konfigurasi sistem yang kritikal. Semua sandaran hendaklah direkodkan dan disimpan di lokasi luar premis *(off-site)* yang selamat. Perkara-perkara berikut hendaklah dipatuhi: a. Sandaran keselamatan bagi semua sistem perisian dan aplikasi hendaklah dilakukan sekurang-kurangnya sekali atau setiap kali versi baharu diperoleh. b. Data dan maklumat hendaklah disandarkan secara berkala mengikut keperluan operasi bagi memastikan tiada kehilangan data penting.	Pentadbir Sistem, Pentadbir Server dan Pentadbir Pangkalan Data

ID	PENERANGAN	PERANAN
	c. Sistem sandaran yang sedia ada hendaklah diuji sekurang-kurangnya sekali setahun untuk memastikan kebolehfungsian, kebolehpercayaan dan keberkesanannya, terutamanya semasa situasi kecemasan atau bencana. d. Sandaran hendaklah dilaksanakan mengikut jadual yang telah ditetapkan sama ada secara harian, mingguan, bulanan atau tahunan berdasarkan tahap kepentingan dan kritikal maklumat yang terlibat.	

8.14 Menyediakan Log *(Logging)*

ID	PENERANGAN	PERANAN
8.14.1	KPN/Agensi hendaklah menyediakan, menyimpan, melindungi, dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat serta peristiwa yang berkaitan dengan keselamatan maklumat. Log sistem ICT merupakan bukti yang didokumenkan dan menjadi turutan kejadian bagi setiap aktiviti yang berlaku dalam sistem. Log ini memainkan peranan penting dalam pemantauan keselamatan, pengesanan insiden serta siasatan sekiranya berlaku pelanggaran keselamatan.	Pentadbir Sistem, CSIRT KPN/Agensi

ID	PENERANGAN	PERANAN
	Log yang direkodkan hendaklah mengandungi maklumat berkaitan, termasuk: a. Pengenalpastian terhadap sebarang cubaan capaian yang tidak dibenarkan. b. Aktiviti yang tidak normal. c. Aktiviti yang mencurigakan atau tidak dapat dijelaskan. Log hendaklah disimpan dalam tempoh minimum dua (2) tahun. Selain itu, kawalan keselamatan log juga perlu dilaksanakan bagi menjamin integriti dan kerahsiaan maklumat yang direkodkan. Jenis-jenis fail log yang perlu diaktifkan bagi Server *(server)* dan aplikasi adalah seperti berikut: a. Fail log sistem pengoperasian; b. Fail log perkhidmatan (contoh: web, e-mel); c. Fail log aplikasi *(audit trail);* dan d. Fail log rangkaian (contoh: suis, tembok api *(firewall),* Sistem Pencegahan Pencerobohan (IPS)).	

8.15 Aktiviti Pemantauan *(Monitoring Activities)*

ID	PENERANGAN	PERANAN
8.15.1	Aktiviti pemantauan dilaksanakan bagi mengesan tingkah laku yang tidak normal (anomali) dan mengenal pasti kemungkinan berlakunya insiden keselamatan maklumat. Pemantauan yang berkesan dapat membantu dalam pengesanan awal, tindak balas segera, serta pencegahan terhadap ancaman keselamatan siber. Perkara-perkara yang perlu dipantau secara berterusan merangkumi, tetapi tidak terhad kepada: a. **Trafik rangkaian masuk *(inbound)* dan keluar *(outbound)*** Termasuk pemantauan trafik ke dan dari sistem, aplikasi serta Server, bagi mengesan sebarang corak trafik luar biasa atau tidak sah. b. **Capaian kepada sistem dan peralatan kritikal** Memantau aktiviti capaian ke atas sistem, Server, peralatan rangkaian, sistem pemantauan serta aplikasi yang dikategorikan sebagai kritikal. c. **Fail konfigurasi dan capaian pentadbir** Mengawasi perubahan terhadap fail konfigurasi rangkaian serta semua capaian yang dilakukan oleh pengguna bertaraf pentadbir ke atas sistem kritikal.	Pentadbir Sistem, CSIRT KPN/Agensi

ID	PENERANGAN	PERANAN
	d. **Log daripada peralatan keselamatan** Memantau log yang dijana oleh sistem keselamatan seperti antivirus, *firewall*, sistem pengesanan dan pencegahan pencerobohan (IDS/IPS), dan lain-lain. e. **Log peristiwa sistem dan rangkaian** Menilai log peristiwa untuk mengenal pasti aktiviti yang mencurigakan, percubaan capaian tanpa kebenaran atau perubahan luar jangka. f. **Integriti kod sistem atau aplikasi** Memastikan kod yang digunakan telah disahkan untuk pelaksanaan dan tidak diubah tanpa kebenaran. g. **Penggunaan prestasi sumber sistem** Memantau penggunaan sumber seperti penggunaan prestasi sumber (*Central Processing Unit* (CPU), h*ard drives*, *Random Access Memory* (RAM), and *network bandwidth* untuk mengesan penggunaan luar biasa atau penyalahgunaan sumber.	

8.16 Penyeragaman Jam *(Clock Synchronisation)*

ID	PENERANGAN	PERANAN
8.16.1	Semua sistem pemprosesan maklumat yang berada dalam domain KPN/Agensi domain keselamatan hendaklah diseragamkan mengikut **Waktu Piawai Malaysia *(Malaysia Standard Time* - MST).** Penetapan masa sistem hendaklah menggunakan sumber masa yang sah dan diluluskan, seperti Server *Network Time Protocol* (NTP) SIRIM, terutamanya bagi sistem yang tergolong dalam persekitaran Jaringan Wujud Padu (JWP) atau domain keselamatan. Penyelarasan waktu yang konsisten adalah penting untuk tujuan berikut: a. Membolehkan korelasi dan analisis yang tepat terhadap kejadian atau insiden keselamatan maklumat. b. Menyokong proses audit, forensik digital, dan penyiasatan insiden secara berkesan. c. Memastikan ketepatan masa dalam semua log sistem, aplikasi, dan peralatan rangkaian bagi tujuan pengesanan dan pelaporan insiden. KPN/Agensi hendaklah memastikan: a. Semua sistem hendaklah dikonfigurasi agar masa	Pentadbir Sistem, CSIRT KPN/Agensi

ID	PENERANGAN	PERANAN
	diselaraskan secara automatik. b. Sumber masa yang digunakan adalah dipercayai, berpusat dan dipantau. c. Mekanisme pemantauan bagi memastikan penyeragaman waktu sentiasa berfungsi dengan baik di semua peringkat sistem.	

8.17 Penggunaan Program Utiliti Khas *(Use of Privileged Utility Programs)*

ID	PENERANGAN	PERANAN
8.17.1	Program utiliti khas ialah perisian atau perintah yang mempunyai keupayaan tinggi dan boleh memberikan akses terus kepada sumber sistem atau fungsi kritikal. Penggunaan program ini perlu dikawal rapi bagi mengelakkan penyalahgunaan, pelanggaran keselamatan, atau pencerobohan sistem. KPN/Agensi hendaklah mematuhi panduan berikut dalam pengurusan dan penggunaan program utiliti khas: a. **Menghadkan bilangan pengguna yang dibenarkan** Hanya pengguna yang sah dan diberi kuasa sahaja dibenarkan untuk menggunakan program utiliti khas. b. **Penggunaan ID yang unik dan boleh dikesan** Setiap pengguna yang diberi kebenaran hendaklah menggunakan ID yang unik	Pentadbir Sistem, CSIRT KPN/Agensi

ID	PENERANGAN	PERANAN
	bagi tujuan pengesahan, penjejakan dan audit. c. **Pengenalpastian dan pendokumentasian** Semua program utiliti yang digunakan hendaklah dikenalpasti dan direkodkan dalam inventori serta didokumenkan dengan jelas. d. **Penggunaan secara luar jangka *(ad-hoc)* dibenarkan secara terkawal** Penggunaan program utiliti secara sementara atau ad-hoc hanya dibenarkan dengan kebenaran khusus dan direkodkan untuk tujuan audit. e. **Penghapusan program utiliti yang tidak berkaitan** Program utiliti yang tidak digunakan atau tidak berkaitan dengan fungsi sistem hendaklah dihapuskan atau dinyahaktifkan. f. **Kawalan ke atas ketersediaan program utiliti** Program utiliti hendaklah hanya tersedia pada persekitaran atau sistem yang memerlukannya, dan tidak boleh diakses secara meluas. g. **Penyimpanan log penggunaan** Log penggunaan program utiliti hendaklah disimpan dan dipantau bagi mengesan sebarang penyalahgunaan atau	

ID	PENERANGAN	PERANAN
	aktiviti mencurigakan. h. **Had ke atas program yang membebankan rangkaian** Penggunaan program utiliti yang boleh menjejaskan prestasi rangkaian, seperti penggunaan bandwidth yang tinggi, hendaklah dihadkan atau dikawal.	

8.18 Pemasangan Perisian pada Sistem Pengoperasian *(Installation of Software on Operational Systems)*

ID	PENERANGAN	PERANAN
8.18.1	Prosedur kawalan pemasangan perisian pada sistem operasi hendaklah dilaksanakan. Setelah mendapat kelulusan daripada pegawai yang diberi kuasa, langkah-langkah berikut mesti dipatuhi: a. Sediakan pelan pemulihan *(rollback)* sebelum buat apa-apa perubahan pada sistem, perisian atau tetapan. b. Aplikasi dan sistem operasi hanya boleh digunakan selepas diuji dan disahkan berfungsi dengan baik. c. Setiap perubahan pada sistem dan perisian mesti direkod dan disimpan dengan baik. d. Kemas kini sistem operasi hanya boleh dibuat oleh Pentadbir ICT yang terlatih dengan kebenaran pengurusan.	Pengurus ICT dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	e. Hanya fail boleh laksana *(executable)* yang diluluskan boleh dipasang. Jangan pasang perisian pembangunan atau penyusun *(compiler).* f. Pastikan semua pustaka *(library)* program dikemas kini supaya serasi. g. Guna sistem kawalan konfigurasi untuk kawal semua perisian dan dokumen berkaitan. h. Simpan versi lama perisian bersama maklumat penting seperti tetapan, panduan, dan perisian sokongan, sebagai persediaan jika berlaku masalah di masa hadapan.	
8.18.1	**Sekatan ke atas Pemasangan Perisian *(Restriction on Software Installation)*** Peraturan pemasangan perisian oleh pengguna mesti disediakan dan dikuatkuasakan. Pengguna hendaklah mematuhi perkara berikut: a. Hanya perisian yang diluluskan dibenarkan digunakan oleh warga pembekal, pakar runding, dan mana-mana pihak yang terlibat dengan perkhidmatan ICT. b. Hanya perisian tulen, berdaftar dan sah di sisi undang-undang boleh dipasang dan digunakan. c. Setiap perisian mesti diimbas	Pentadbir Sistem, warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT KPN/Agensi

ID	PENERANGAN	PERANAN
	dengan antivirus sebelum dipasang atau digunakan dalam sistem.	

8.19 Kawalan Rangkaian *(Network Control)*

ID	PENERANGAN	PERANAN
8.19.1	Kawalan ke atas infrastruktur rangkaian perlu dilaksanakan bagi melindungi maklumat dan perkhidmatan ICT daripada sebarang capaian tidak sah. Perkara-perkara berikut mesti dipatuhi: a. Pastikan operasi rangkaian dilindungi daripada sebarang pengubahsuaian tanpa kebenaran. b. Letakkan peralatan rangkaian di lokasi yang selamat dan terlindung daripada risiko seperti banjir, gegaran dan habuk. c. Kawal capaian ke peralatan rangkaian – hanya pengguna yang diberi kebenaran dibenarkan. d. Laksanakan *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi semua peralatan rangkaian. e. Pasang dan selenggara *firewall* oleh Pentadbir Rangkaian yang dilantik. f. Semua trafik keluar dan masuk	Pengurus ICT dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	rangkaian mesti melalui firewall di bawah kawalan KPN/Agensi. g. Penggunaan perisian *sniffer* atau *network analyser* pada komputer pengguna adalah dilarang kecuali dengan kebenaran ICTSO. h. *Pasang Intrusion Prevention System* (IPS) bagi menghalang pencerobohan dan ancaman keselamatan. i. Gunakan *Web Content Filtering* di Internet Gateway untuk menyekat akses kepada kandungan yang tidak dibenarkan. j. Sambungan rangkaian selain daripada yang dikawal oleh KPN/Agensi adalah tidak dibenarkan. k. Semua pengguna mesti guna rangkaian rasmi KPN/Agensi sahaja. Penggunaan modem adalah dilarang. l. Pantau dan kawal penggunaan *wireless* LAN. m. Semua perjanjian perkhidmatan rangkaian mesti patuhi *Service Level Assurance* (SLA) yang ditetapkan. n. Pasang antara muka yang sesuai bagi sambungan antara rangkaian KPN/Agensi rangkaian jabatan lain dan rangkaian awam.	

ID	PENERANGAN	PERANAN
	o. Laksana mekanisme pengesahan untuk pengguna dan peralatan yang sah digunakan. p. Kawal capaian pengguna kepada perkhidmatan rangkaian ICT yang dibenarkan sahaja. q. Kawal capaian fizikal dan logikal ke port diagnostik dan peralatan konfigurasi jarak jauh. r. Kawal sambungan ke rangkaian terutamanya bagi kemudahan yang dikongsi atau merentas sempadan organisasi. s. Laksanakan kawalan laluan *(routing control)* mengikut peraturan KPN/Agensi . t. Pastikan semua peralatan yang disambung ke rangkaian bebas virus dan mempunyai antivirus sah. u. Capaian rangkaian mesti ikut kategori yang ditetapkan: Intranet, Internet, dan DMZ. v. Sistem dalam rangkaian Internet tidak boleh dicapai terus dari luar. w. Pihak ketiga hanya dibenarkan akses ke rangkaian Intranet untuk tujuan pembangunan	

ID	PENERANGAN	PERANAN
	atau penyelenggaraan sistem, dengan kebenaran rasmi. x. Akses ke rangkaian *wireless* mesti dikawal mengikut kategori pengguna.	

8.20 Keselamatan Perkhidmatan Rangkaian *(Security of Network Services)*

ID	PENERANGAN	PERANAN
8.20.1	Pengurusan bagi semua perkhidmatan rangkaian *(inhouse* atau *outsource)* yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan. Aspek keselamatan perkhidmatan rangkaian yang perlu mengambil kira seperti berikut: a. Menggunakan teknologi keselamatan perkhidmatan rangkaian seperti pengesahan identiti, kawalan akses atau penggunaan enkripsi. b. Memastikan peralatan rangkaian mematuhi polisi parameter yang ditetapkan bagi menjamin keselamatan sambungan rangkaian. c. Memastikan kawalan akses kepada perkhidmatan rangkaian dan sistem aplikasi mengikut peranan yang diluluskan.	ICTSO, Pengurus ICT, Pentadbir Sistem dan Pembekal

ID	PENERANGAN	PERANAN
	d. Memastikan trafik rangkaian dipantau dan dikawal oleh peralatan keselamatan. e. Menggunakan penapisan kandungan laman web bagi mengawal akses ke laman web yang tidak dibenarkan.	
8.20.2	**Peralatan dalam rangkaian** Bagi memastikan bahawa peralatan yang disambungkan kepada rangkaian KPN/Agensi tidak menjejaskan keselamatan maklumat dan capaian, perkara-perkara berikut hendaklah dipatuhi: a. Semua peralatan perlu disahkan bebas daripada virus dan perisian *antivirus* yang sah hendaklah dipasang dan masih aktif sepanjang masa. b. Pengguna perlu menggunakan ID dan katalaluan yang sah untuk disambungkan ke rangkaian. c. Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan konfigurasi yang ditetapkan oleh pentadbir rangkaian.	Pentadbir Rangkaian

8.21 Pengasingan dalam Rangkaian *(Segregation in Networks)*

ID	PENERANGAN	PERANAN
8.21.1	Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian KPN/Agensi.Perkara yang perlu dipatuhi adalah seperti berikut: a. Menyediakan segmen yang hanya untuk kegunaan warga KPN/Agensi. b. Menetapkan segmen yang berbeza bagi pengguna biasa, pentadbir, Server, sistem aplikasi dan pihak ketiga. c. Mengasingkan akses rangkaian mengikut tahap kritikal dan sensitiviti atau lain-lain keperluan. d. Memastikan penggunaan peralatan keselamatan seperti *firewall* atau *router* bagi mengawal segmen rangkaian. e. Melaksanakan polisi kawalan akses melalui *gateway* berdasarkan keperluan dan klasifikasi maklumat. f. Mengasingkan rangkaian tanpa wayar dengan rangkaian dalaman kecuali dengan menggunakan kawalan keselamatan seperti *firewall*. g. Mengasingkan akses rangkaian tanpa wayar untuk pelawat dan Warga KPN/Agensi.	ICTSO, Pengurus ICT dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	h. Mengawal akses kepada peralatan rangkaian bagi pengguna yang dibenarkan sahaja. i. Mengemaskinikan hak akses pengguna dan pentadbir sekiranya berlaku perubahan tanggungjawab.	
8.21.2	Kawalan penyaringan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat akses ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi organisasi daripada sebarang ancaman keselamatan siber.Perkara yang perlu dipatuhi adalah seperti berikut: a. Menyekat alamat IP atau *domain* laman web yang tidak sah. b. Memantau laman web yang mempunyai fungsi muat naik maklumat. c. Menyekat laman web berbahaya seperti *phishing* dan *malicious*. d. Mengemaskini pangkalan data (*signature database)* peralatan keselamatan web melalui sumber yang sahih *(threat intelligence).* e. Menyekat laman web perkongsian maklumat yang tidak sah *(illegal).*	Pentadbir Rangkaian

ID	PENERANGAN	PERANAN
	f. Memberikan latihan teknikal kepada kepada warga teknikal mengenai pengendalian peralatan laman web. g. Memberikan program kesedaran kepada pengguna mengenai tatacara akses laman web yang selamat.	

8.22 Dasar Pembangunan Sistem yang Selamat *(Secure Development Policy)*

ID	PENERANGAN	PERANAN
8.22.1	Peraturan dan garis panduan pembangunan perisian dan sistem hendaklah disediakan dan dipatuhi oleh semua pihak yang terlibat dalam pembangunan ICT organisasi. Antara perkara yang perlu diberi perhatian ialah: a. Aspek keselamatan mesti diambil kira dalam pembangunan perkhidmatan, infrastruktur, perisian dan sistem. b. Asingkan persekitaran pembangunan, pengujian dan pengeluaran *(production)* bagi mengelakkan gangguan kepada sistem sebenar. c. Gunakan panduan keselamatan pembangunan sistem sepanjang kitar hayat pembangunan (SDLC), termasuk:	ICTSO, Pengurus ICT dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	i. Metodologi pembangunan yang menekankan keselamatan; ii. Garis panduan pengekodan selamat mengikut bahasa pengaturcaraan yang digunakan. d. Masukkan keperluan keselamatan dalam setiap fasa: spesifikasi, reka bentuk dan pengurusan projek. e. Melaksanakan ujian keselamatan seperti: i. Ujian penembusan *(penetration test);* ii. Semakan kod *(code review);* iii. Ujian pepijat *(bug testing)* selepas setiap kemas kini. f. Simpan kod sumber dan konfigurasi sistem aplikasi di tempat yang selamat dan dikawal. g. Pastikan setiap perubahan versi sistem aplikasi dikawal dengan langkah keselamatan yang sesuai. h. Sediakan latihan keselamatan aplikasi untuk pembangun bagi meningkatkan kemahiran mengenal pasti dan membaiki kelemahan aplikasi. i. Ambil kira keperluan lesen	

ID	PENERANGAN	PERANAN
	perisian dan pertimbangkan alternatif lain yang sah untuk kawalan kos yang lebih berkesan. j. Pastikan pembangunan oleh pihak ketiga memasukkan elemen pembangunan selamat *(secure development life cycle)* dalam kontrak dan perjanjian kerja.	
8.22.2	Keperluan keselamatan sistem aplikasi yang perlu diambil kira adalah seperti berikut: a. Memastikan pengguna mempunyai tahap akses yang dibenarkan. b. Mengenalpasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi. c. Membezakan had akses kepada data dan fungsi dalam sistem aplikasi. d. Ketahanan terhadap ancaman perisian hasad atau gangguan pihak yang tidak dibenarkan. e. Memastikan perundangan dan peraturan dipatuhi bagi transaksi yang dijana, diproses, dilengkapkan atau disimpan. f. Menetapkan keperluan privasi bagi pihak yang terlibat. g. Memastikan maklumat rahsia rasmi dilindungi.	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	h. Memastikan data yang diproses dan dipindahkan dilindungi. i. Memastikan komunikasi antara semua pihak dienkripsi dengan selamat. j. Melaksanakan pengesahan input. k. Mengawal kelulusan yang dijana oleh Sistem Aplikasi seperti mengehadkan kelulusan atau kelulusan melebihi satu orang pelulus. l. Mengawal kebenaran untuk akses kepada output yang dihasilkan. m. Mengehadkan kandungan medan *free text* bagi mengawal kapasiti storan. n. Melaksanakan pemantauan dan merekodkan log transaksi ke atas proses kerja. o. Memastikan kawalan keselamatan sistem aplikasi seperti penggunaan perisian log atau sistem pengesanan kebocoran data. p. Pengendalian mesej ralat.	

8.23 Prinsip Kejuruteraan Sistem yang Selamat *(Secure System Engineering Principles)*

ID	PENERANGAN	PERANAN
8.23.1	Prinsip kejuruteraan yang selamat perlu dilaksanakan bagi memastikan perlindungan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a. Menyediakan kawalan keselamatan yang diperlukan untuk melindungi maklumat dan sistem aplikasi daripada ancaman yang dikenalpasti. b. Mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan. c. Mengenalpasti keperluan kawalan keselamatan yang akan dilaksanakan. d. Melaksanakan kawalan keselamatan terhadap individu yang berkaitan. e. Memastikan prinsip kejuruteraan mengaplikasikan reka bentuk keselamatan *(security architecture).* f. Mempunyai kepakaran untuk pembangunan dan menyelenggara sistem aplikasi selari dengan teknologi yang digunakan atau dipilih. g. Mengambil kira keperluan kos, masa dan cabaran dalam memenuhi keperluan	Pentadbir Sistem, Pengurus ICT

ID	PENERANGAN	PERANAN
	keselamatan. h. Menggunapakai konsep amalan terbaik *(best practices).* i. Melaksanakan *Security Posture Assessment* (SPA) dan *hardening* ke atas sistem aplikasi yang kritikal. KPN/Agensi perlu mengambil kira Prinsip *Zero Trust* seperti berikut: a. Kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian; atau b. Menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi; atau c. Memastikan sistem aplikasi menggunakan fungsi enkripsi; atau d. Menyemak dan mengesahkan semua permohonan akses yang diterima; atau e. Memberikan kategori akses paling minimum kepada pengguna.	

8.24 Kawalan Capaian Kepada Kod Sumber *(Source Code)*

ID	PENERANGAN	PERANAN
8.24.1	Kawalan capaian kepada kod sumber program perlu dilaksanakan bagi mengelakkan risiko seperti kecurian, pengubahsuaian atau pemadaman tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian adalah hak milik KPN/Agensi. Perkara yang perlu dipatuhi termasuk tetapi tidak terhad kepada: a. **Perancangan Sebelum Pengekodan** i. Gunakan pengekodan selamat mengikut peraturan dan keperluan semasa, sama ada pembangunan secara dalaman *(in-house)* atau oleh pihak luar *(outsource).* ii. Rujuk kelemahan dan amalan terdahulu untuk elakkan pengulangan kesilapan keselamatan. iii. Gunakan *Integrated Development Environment* (IDE) yang menyokong pengekodan selamat. iv. Jalankan pembangunan dalam persekitaran pembangunan khas, bukan pada sistem pengeluaran *(production).* v. Gunakan perisian pembangunan yang terkini dan sah.	Pentadbir Sistem, ICTSO, Pembangun Sistem Aplikasi

ID	PENERANGAN	PERANAN
	b. **Perancangan Semasa Pengekodan** i. Gunakan teknik dan struktur pengekodan yang selamat mengikut bahasa pengaturcaraan yang digunakan. ii. Kenal pasti dan baiki kelemahan kod sumber yang boleh dieksploitasi. iii. Pastikan perisian yang digunakan masih disokong dan belum tamat sokongan *(End of Support).* iv. Melaksanakan ujian keselamatan dan tindakan pembetulan secara berkala. v. Pastikan sistem boleh berintegrasi dengan sistem maklumat lain secara selamat. c. **Semakan dan Penyelenggaraan** vi. Kemas kini *patches* dan *security updates* secara berkala. vii. Ambil tindakan segera terhadap kelemahan keselamatan yang dilaporkan. viii. Rekod dan semak ralat serta cubaan serangan untuk penambahbaikan kod. ix. Lindungi kod sumber daripada akses tidak sah menggunakan sistem kawalan versi *(version control).* d. **Penggunaan *Libraries* Luaran**	

ID	PENERANGAN	PERANAN
	Jika menggunakan libraries atau komponen pihak ketiga: i. Gunakan versi terkini dan disokong. ii. Pastikan komponen seperti pengesahan kriptografi adalah stabil dan selamat. iii. Semak dan patuhi lesen serta keselamatan komponen. iv. Pastikan *libraries* diperoleh dari sumber yang sah dan boleh diselenggara. v. Sediakan dokumentasi dan sumber rujukan untuk sokongan jangka panjang. e. **Penambahbaikan Perisian *(Software Package Enhancement)*** Jika perlu menaik taraf atau menambah baik perisian: i. Nilai risiko terhadap fungsi sedia ada dan integriti sistem. ii. Dapatkan persetujuan bertulis daripada pihak ketiga jika berkaitan. iii. Pertimbangkan keperluan perubahan versi terkini. iv. Nilai implikasi jika penyelenggaraan diserahkan kepada KPN/Agensi. v. Pastikan keserasian dengan perisian lain dalam persekitaran organisasi.	

8.25 Pengujian Keselamatan Sistem *(System Security Testing)*

ID	PENERANGAN	PERANAN
8.25.1	Pengujian keselamatan hendaklah merangkumi perkara berikut: a. Fungsi keselamatan sistem aplikasi hendaklah diuji semasa fasa Pembangunan seperti pengesahan pengguna, kawalan akses dan pengekodan selamat. b. Konfigurasi keselamatan yang melibatkan sistem pengoperasian, *firewalls* dan komponen keselamatan lain hendaklah diuji. c. *Security Posture Assessment* (SPA) hendaklah dilaksanakan ke atas sistem aplikasi kritikal. d. Melaksanakan semakan dan pengesahan ke atas *output* data yang dihasilkan oleh sistem aplikasi.	Pentadbir Sistem, ICTSO

8.26 Pembangunan oleh Khidmat Luaran *(Outsourced Software Development)*

ID	PENERANGAN	PERANAN
8.26.1	KPN/Agensi hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Memastikan perjanjian lesen, dan kod sumber menjadi hak milik kerajaan bagi sistem	Pengurus ICT, ICTSO, Pembangun Sistem Aplikasi

ID	PENERANGAN	PERANAN
	aplikasi yang dibangunkan untuk KPN/Agensi. b. Memastikan spesifikasi perolehan mengandungi klausa berhubung keperluan keselamatan reka bentuk, keselamatan pengaturcaraan, pengujian, pensijilan keselamatan produk, ketersediaan kod sumber, keperluan pelupusan data, keutamaan terhadap teknologi dan kepakaran tempatan serta keperluan kompetensi pasukan pembangunan. c. Menyediakan penilaian keselamatan oleh pihak ketiga seperti terkandung dalam Surat Pekeliling Am Bilangan 4 2024 : Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam. d. Melaksanakan pengujian penerimaan untuk memastikan kualiti dan output memenuhi keperluan. e. Memastikan penilaian risiko keselamatan dan privasi di tahap minimum yang boleh diterima. f. Memastikan pengujian keselamatan, kelemahan yang dikenal pasti dan tindakan pembetulan dilaksanakan adalah mencukupi sebelum penyerahan projek.	

ID	PENERANGAN	PERANAN
	g. Menguatkuasakan *Liquidated Ascertained Damages* (LAD)/bon perjanjian sekiranya pihak ketiga tidak memenuhi perkhidmatan. h. Memasukkan klausa dalam kontrak yang membenarkan pelaksanaan audit terhadap proses pembangunan dan kod sumber. i. Melaksanakan keperluan keselamatan untuk persekitaran pembangunan. j. Mengambil kira perundangan yang berkuatkuasa seperti *Personal Data Act*. k. Sistem aplikasi perlu diangkat untuk kelulusan JPICT sebelum dibangunkan.	

8.27 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi *(Separation of Development, Test and Operational Facilities)*

ID	PENERANGAN	PERANAN
8.27.1	Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Mengasingkan persekitaran sebenar dengan pembangunan dalam domain yang berbeza seperti virtual atau fizikal.	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	b. Menetapkan, merekodkan dan melaksanakan peraturan serta pengesahan untuk penggunaan sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran sebenar. c. Melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam persekitaran sebenar. d. Tidak menggunakan maklumat sebenar pada persekitaran pembangunan atau persekitaran pengujian kecuali dengan kawalan keselamatan. e. Memastikan *compilers, editor* dan *tools* pembangunan atau program utiliti lain tidak boleh diakses daripada persekitaran sebenar apabila tidak diperlukan lagi. f. Merekodkan semua penggunaan sumber yang dilaksanakan. g. Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti. Persekitaran pengujian dan pembangunan perlu dilindungi dengan mengambilkira perkara-perkara berikut : a. Mengemaskini *patches*,	

ID	PENERANGAN	PERANAN
	pembangunan sistem aplikasi, integrasi dan tools pengujian seperti *builders*, *integrators*, *compilers*, sistem konfigurasi dan *libraries*. b. Memastikan keselamatan konfigurasi sistem aplikasi dan operasi perisian yang selamat. c. Memantau dan memastikan kawalan akses persekitaran. d. Memantau kawalan perubahan persekitaran dan kod yang disimpan. e. Menyediakan sandaran *(backup)* mengikut persekitaran.	

8.28 Pengurusan Perubahan *(Change Management)*

ID	PENERANGAN	PERANAN
8.28.1	Perubahan dalam organisasi, business process, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu.	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
8.28.2	**Prosedur Kawalan Perubahan Sistem *(System Change Control Procedures)*** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	Pengurus ICT dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan KPN/Agensi. c. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal. d. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja. e. Capaian kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
8.28.3	**Penilaian Teknikal Sistem Aplikasi Selepas *Perubahan (Technical Review of Applications After Operating Platform Change*** Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform.	Pentadbir Sistem

ID	PENERANGAN	PERANAN
	b. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. c. Memastikan perubahan yang sesuai dibuat kepada PKP KPN/Agensi dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pengurusan Keselamatan Maklumat.	
8.28.4	**Sekatan Ke atas Perubahan Dalam Pakej Perisian *(Restrictions on Changes to Software Packages)*** Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan perubahan pakej perisian ini mengambilkira aspek keselamatan maklumat. b. Perubahan pakej perisian ini hanya dilaksanakan oleh pihak yang dibenarkan sahaja. c. Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna mengenai perubahan versi pakej perisian. d. Memastikan perubahan pakej perisian ini tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pentadbir Sistem, Pengurus ICT

8.29 Perlindungan Data Ujian *(Protection of Test Data)*

ID	PENERANGAN	PERANAN
8.29.1	Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal bagi memastikan perlindungan ke atas maklumat yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian. b. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian. c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai. d. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar. e. Melindungi maklumat sensitif melalui penyingkiran atau penutupan *(masking)* jika digunakan untuk ujian. f. Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	Pengguna, Pentadbir Sistem, ICTSO

8.30 Kawalan Audit Sistem Maklumat *(Information Systems Audit Controls)*

ID	PENERANGAN	PERANAN
8.32.1	Keperluan dan aktiviti audit yang melibatkan pengesahan sistem operasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan perkhidmatan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Mendapatkan kebenaran untuk capaian kepada sistem aplikasi dan data bagi ujian audit. b. Mendapatkan kebenaran untuk melaksanakan ujian audit berdasarkan kawalan dan skop yang dibenarkan. c. Memastikan data yang dibenarkan hanya berstatus *Read Only* semasa ujian audit dilaksanakan. d. Jika terdapat keperluan capaian lebih daripada *Read Only,* pengujian hendaklah dilaksanakan oleh pentadbir yang dibenarkan bagi membantu juruaudit. e. Memastikan keperluan keselamatan perkakasan juruaudit dipatuhi seperti penggunaan antivirus sebelum kebenaran diberikan. f. Membenarkan capaian kepada sistem fail oleh juruaudit dan menghapuskan data tersebut setelah audit selesai atau melaksanakan kawalan	ICTSO, dan Pentadbir Sistem

ID	PENERANGAN	PERANAN
	keselamatan yang bersesuaian. g. Memastikan penggunaan peralatan audit *(audit tools)* mendapat kelulusan terlebih dahulu. h. Melaksanakan ujian audit diluar waktu bekerja sekiranya menyebabkan gangguan perkhidmatan. i. Menyimpan dan memantau semua akses semasa ujian audit.	

LAMPIRAN A1

AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER
KEMENTERIAN PERPADUAN NEGARA (KPN)

NAMA (HURUF BESAR) : .....

NO. KAD PENGENALAN : .....

JAWATAN : .....

BAHAGIAN : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber KPN; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan tatatertib yang sewajarnya dan tindakan undang-undang yang berkaitan boleh dikenakan ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT,

.....

(Tandatangan & Cop Jawatan)

Kementerian Perpaduan Negara/Agensi

Tarikh : .....

* Polisi Keselamatan Siber KPN boleh dicapai menerusi www.perpaduan.gov.my

LAMPIRAN B

UNDANG-UNDANG, PEKELILING DAN DASAR YANG TERPAKAI

Polisi Keselamatan Siber Kementerian Perpaduan Negara dan Agensi ini hendaklah dibaca bersama dengan akta-akta, warta, pekeliling-pekeliling, surat pekeliling dan peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut;

1. Akta Hak Cipta (Pindaan) Tahun 1997;
2. Akta Jenayah Komputer 1997;
3. Akta Komunikasi dan Multimedia 1998;
4. Akta Rahsia Rasmi 1972;
5. Akta Tandatangan Digital 1997;
6. Akta Keselamatan Siber 2024;
7. Akta Arkib Negara 2003 (Akta 629);
8. Arahan Teknologi Maklumat 2007;
9. Arahan Keselamatan;
10. Arahan Perbendaharaan;
11. Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi
12. Maklumat dan Komunikasi Kerajaan;
13. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan
14. Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
15. Pekeliling Perbendaharaan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan (TPA);
16. Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007;
17. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar
18. Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key
19. Infrastruktur (GPKI)];
20. Pekeliling Transformasi Pentadbiran Awam Bil.3 Tahun 2017 Pengurusan
21. Komunikasi Bersepadu Kerajaan (Government Unified Communication (1GovUC));
22. Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
23. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam;
24. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden
25. Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;

26. Surat Pekeliling Am Bilangan 3 Tahun 2024 Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024;
27. Surat Pekeliling Am Bilangan 4 Tahun 2024 Garis Panduan Penilaian Tahap
28. Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
29. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan;
30. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 November 2007 Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan;
31. Malaysian *Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);
32. Perintah-Perintah Am;
33. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016;
34. Surat Pekeliling Am Bilangan 3 Tahun 2024: Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024.
35. Surat Pekeliling Am Bilangan 7 Tahun 2024 (SPA Bil. 7/2024) yang telah dikeluarkan oleh Agensi Digital Negara pada 16 Julai 2024.
36. Surat Pekeliling Am Bilangan 7 Tahun 2024, Garis Panduan Permohonan Kelulusan Teknikal Dan Pemantauan Projek Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam yang telah dikeluarkan oleh Jabatan Perdana Menteri pada 16 Julai 2024.
37. Pekeliling Am Bilangan 4 Tahun 2022: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.
38. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam.
39. Surat Pekeliling Am Bilangan 5 Tahun 2007 – Pengurusan Rekod Awam;
40. Arahan Setiausaha Majlis Keselamatan Negara (MKN) (Bilangan 1 Tahun 2013)
41. Surat Arahan Ketua Agensi (Bertarikh 1 Jun 2007) Garis Panduan Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (MyGovUC)
42. Garis Panduan Notifikasi Pelanggaran Data *(Data Breach Notification Guideline,* PDPA,2025)
43. Surat Pekeliling Am Bilangan 4 Tahun 2022 (SPA 4/2022): Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam
44. Surat Pekeliling Am Bilangan 4 2024 : Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.

LAMPIRAN C

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan peruntukan Akta Rahsia Rasmi 1972 [Akta88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun. Saya faham bahawa segala rahsia rasmi dan surat rasmi yang saya peroleh dalam perkhidmatan Seri Paduka Baginda Yang di - Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akaun selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan	:	.....
Nama (huruf besar)	:	.....
No. Kad Pengenalan	:	.....
Jawatan	:	.....
Tarikh	:	.....
Disaksikan oleh	:	.....

Tandatangan	:	.....
Nama (huruf besar)	:	.....
No. Kad Pengenalan	:	.....
Jawatan	:	.....
Tarikh	:	.....
Cop Kementerian/Agensi	:	