VERSI 2.0

TERHAD

KEMENTERIAN SUMBER MANUSIA

PERKESO

POLISI KESELAMATAN SIBER

(PKSB)

PERTUBUHAN KESELAMATAN SOSIAL

PENGGUNA LUAR

Polisi Keselamatan Siber
Pertubuhan Keselamatan Sosial (PERKESO)
Kementerian Sumber Manusia

Versi 2.0

TARIKH KUAT KUASA

8 APRIL 2026

Diterbitkan oleh:

Cawangan Keselamatan
Bahagian Khidmat Pengurusan
Ibu Pejabat Pertubuhan Keselamatan Sosial (PERKESO)
Tingkat 11, Menara PERKESO
Jalan Ampang, 50538 Kuala Lumpur
Tel: 03-4264 5000

VERSI DOKUMEN POLISI KESELAMATAN SIBER (PKSB) PERKESO

VERSI	KELULUSAN	ARAHAN PENTADBIRAN	TARIKH KUATKUASA
Versi 1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) PERKESO Bil 3/2022	Bil 6/2022	25 April 2022
Versi 1.1	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) PERKESO Bil 8/2022	Bil 12/2022	13 Disember 2022
Versi 2.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) PERKESO Bil 1/2026	Bil 5/2026	8 April 2026

KANDUNGAN

LAMPIRAN

Format Polisi Keselamatan Siber PERKESO

DP5.1.1 Pelaksanaan Polisi

DP	01	01	01	5.1.1
PKSB PERKESO	Bidang	Objektif mengikut Bidang	Kawalan Objektif Bagi Objektif mengikut Bidang	Kod yang digunakan dalam ISO/IEC 27001:2022

AKRONIM / TERMA / TAKRIFAN

SINGKATAN DAN GLOSARI	KETERANGAN
Antivirus	Perisian yang digunakan untuk mengesan dan membuang *malware*, seperti virus komputer, *adware, backdoors, malicious BHO's, diallers, fraud tools, hijackers, key loggers, malicious LSPs, rootkits, spyware, Trojan horses* dan *worms*.
API	*Application Programming Interface* Satu set arahan pengaturcaraan dan standard untuk akses menerusi aplikasi web menggunakan perisian aplikasi web
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi dan sumber manusia serta premis berkaitan dengan ICT yang di bawah tanggungjawab PERKESO.
Backup	Sandaran Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus.
Bandwidth	Jalur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contoh: video streaming dan persidangan video (*teleconference)*.
BAR	Bahagian Audit dan Risiko PERKESO
BCP / PKP	*Business Continuity Management* atau Pelan Kesinambungan Perkhidmatan 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.
BICT	Bahagian ICT PERKESO
Bilik Server	Ruang ICT di premis PERKESO yang menempatkan pelayan, peralatan rangkaian, sistem storan dan komponen sokongan ICT berskala kecil hingga sederhana
BKP	Bahagian Khidmat Pengurusan PERKESO
CSIRT	*Cyber Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu PERKESO menguruskan pengendalian insiden keselamatan siber di PERKESO.

SINGKATAN DAN GLOSARI	KETERANGAN
CDO	*Chief Digital Officer* Ketua Pegawai Digital, iaitu pegawai yang dilantik untuk mengetuai, menyelaras, menyelia serta memantau keseluruhan pelaksanaan pendigitalan, pengurusan ICT, keselamatan siber dan tadbir urus data serta bertindak sebagai penasihat utama kepada Ketua Jabatan dalam semua urusan berkaitan teknologi maklumat dan transformasi digital dengan PERKESO.
CGSO	*Chief Government Security Office* Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia
Denial of Service	Halangan pemberian perkhidmatan
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 E-mel.
DRP / ITDRP	*Disaster Recovery Plan* / *IT Disaster Recovery Plan* Pelan Pemulihan Bencana IT, ialah dokumen strategik dan prosedur terperinci yang disediakan oleh organisasi untuk memastikan sistem teknologi maklumat (IT) dapat dipulihkan dan beroperasi semula selepas berlakunya gangguan besar atau bencana. Tujuan utama pelan ini adalah untuk meminimumkan kesan gangguan terhadap operasi PERKESO dan memastikan kesinambungan perkhidmatan kritikal.
E-mel	Mel Elektronik Maklumat atau mesej yang dihantar secara elektronik dari satu terminal komputer ke terminal komputer yang lain.
Enkripsi	*Encryption* Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui E-mel termasuk penyalahgunaan/ pencurian identiti dan pencurian/penipuan maklumat.

SINGKATAN DAN GLOSARI	KETERANGAN
ICT	*Information and Communication Technology* atau Teknologi Maklumat dan Komunikasi 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.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Mekanisme keselamatan ini merujuk kepada perisian atau perkakasan yang digunakan untuk memantau, mengesan dan bertindak balas terhadap aktiviti tanpa kebenaran, kesilapan atau aktiviti berbahaya dalam persekitaran teknologi maklumat, sama ada melalui pemantauan berasaskan hos atau rangkaian, bergantung kepada jenis data dan tingkah laku sistem yang dianalisis.
Insiden Keselamatan Siber	Musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar PKSB sama ada yang ditetapkan secara tersurat atau tersirat.
Internet	Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Mekanisme keselamatan rangkaian ini merujuk kepada perkakasan keselamatan komputer yang memantau aktiviti rangkaian dan/atau sistem bagi mengesan perisian berbahaya atau aktiviti berniat jahat, serta berkeupayaan bertindak balas secara automatik dengan menyekat atau menghalang serangan dan kod berniat jahat bagi melindungi keselamatan sistem dan rangkaian organisasi.
ISMS	*Information Security Management System atau* Sistem Pengurusan Keselamatan Maklumat. ISO/IEC 27001 (ISMS) menyatakan keperluan untuk mewujud, mengoperasi, memantau, mengkaji semula, menyenggara dan memperbaiki Sistem Pengurusan Keselamatan Maklumat organisasi. Pematuhan kepada standard/ piawaian ISMS ini menunjukkan bahawa sistem pengurusan organisasi perlu memastikan kerahsiaan, integriti dan ketersediaan

SINGKATAN DAN GLOSARI	KETERANGAN
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.
Kawasan Larangan	Kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan.
Kelulusan	Kuasa melulus ini hendaklah diberikan kepada individu yang berkelayakan bagi menjamin kawalan dan integriti maklumat sentiasa terpelihara.
Koordinator Pasukan Keselamatan Maklumat	Berperanan penting dalam menyelaras dan memastikan pelaksanaan aktiviti keselamatan maklumat berjalan lancar melalui kerjasama semua peringkat pengguna di PERKESO.
Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.
LAN	*Local Area Network* atau Rangkaian Setempat 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 *external hard drive, flash disk, 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.
PERKESO	Pertubuhan Keselamatan Sosial
Pusat Data	Kemudahan ICT kritikal PERKESO yang direka bentuk untuk menempatkan, mengendalikan dan melindungi infrastruktur teknologi organisasi termasuk pelayan, sistem storan, peralatan rangkaian, pangkalan data serta aplikasi teras utama.

SINGKATAN DAN GLOSARI	KETERANGAN
Pemilik Sistem	Pemilik bisnes (*business owner*) bagi sistem yang dibangunkan atau Bahagian / Cawangan / Unit di bawah PERKESO yang paling banyak memiliki data dalam sesuatu sistem.
Pemegang Taruh	Semua pihak yang mempunyai kepentingan dengan Jabatan.
Pentadbir Pasukan Keselamatan Maklumat	Pegawai atau staf yang dilantik dalam pasukan keselamatan maklumat PERKESO untuk menjalankan tugas pentadbiran teknikal, pemantauan, pematuhan dan pelaksanaan kawalan keselamatan maklumat dalam bidang tanggungjawab masing-masing.
Pengguna Luar	Individu, syarikat atau organisasi yang dibenarkan mengakses rangkaian, sistem atau data organisasi melalui kelayakan akses yang diluluskan dan tertakluk kepada dasar keselamatan ICT PERKESO.
Pentadbir Sistem ICT	Pentadbir yang membangunkan, melaksanakan dan menyelenggara sistem aplikasi, laman web, media sosial dan aplikasi mudah alih.
Peralatan ICT	Merujuk kepada perkakasan dan perisian ICT (*hardware* dan *software*) yang digunakan dalam teknologi maklumat dan komunikasi
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), pencetak, pengimbas dan sebagainya.
Perisian	Set aturcara 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 semua komponen fizikal peralatan ICT yang boleh dilihat dan disentuh.
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.

SINGKATAN DAN GLOSARI	KETERANGAN
PKSB	Polisi Keselamatan Siber, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT dan ruang siber
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
Salinan Bercetak	Salinan bercetak merujuk kepada dokumen atau maklumat yang telah dicetak di atas kertas, sama ada menggunakan pencetak, mesin fotostat atau alat cetakan lain, daripada versi asal yang berbentuk digital atau elektronik.
Salinan Digital	Salinan digital merujuk kepada dokumen atau fail yang disimpan, dihantar atau dipaparkan dalam bentuk elektronik, lazimnya dalam format seperti PDF, DOCX, JPEG, PNG, atau seumpamanya.
Secure Sockets Layer (SSL)	Protokol keselamatan standard yang digunakan untuk mewujudkan pautan yang disulitkan antara pelayan web dan pelayar web (atau klien lain) bagi memastikan semua data yang dihantar kekal peribadi dan selamat
Server	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 berbagai kegiatan sehari-hari
Sistem ICT	Merangkumi Sistem Aplikasi, Pentadbiran Server, 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.
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.

1.0 PENDAHULUAN

1.1 Pengenalan

Polisi Keselamatan Siber (PKSB), Pertubuhan Keselamatan Sosial (PERKESO) ialah dokumen yang menetapkan hala tuju yang jelas bagi PERKESO dalam usaha memastikan keselamatan maklumat secara menyeluruh. Polisi ini telah mendapat kelulusan rasmi serta komitmen penuh daripada pengurusan tertinggi untuk pelaksanaan yang efektif. Polisi ini disediakan dengan tujuan untuk melindungi kerahsiaan, integriti, dan ketersediaan maklumat di PERKESO merangkumi satu set arahan, peraturan, garis panduan, dan amalan yang ditetapkan untuk melindungi maklumat serta data yang sensitif dan kritikal daripada capaian yang tidak sah, kehilangan, atau pendedahan yang tidak dibenarkan. PKSB PERKESO ini mentakrifkan kawalan keselamatan yang bersesuaian berdasarkan dasar, pekeliling, garis panduan kerajaan semasa yang berkuat kuasa serta mengikut amalan terbaik keselamatan yang relevan. Polisi ini terpakai kepada semua sistem dan persekitaran maklumat PERKESO, memastikan perlindungan menyeluruh terhadap ancaman siber yang semakin kompleks.

1.2 Tujuan

PKSB PERKESO dibangunkan untuk mewujudkan rangka kerja yang komprehensif dalam melindungi aset maklumat PERKESO daripada ancaman dan kerentanan yang mungkin timbul. Polisi ini bertujuan untuk memastikan kerahsiaan, integriti, dan ketersediaan maklumat, sambil mematuhi keperluan undang-undang dan peraturan yang relevan. Dengan wujudnya PKSB PERKESO ini, diharapkan pengurusan keselamatan data dan maklumat di jabatan ini akan menjadi lebih efisien dan efektif, serta dapat meningkatkan tahap jaminan keselamatan yang lebih tinggi.

1.3 Objektif

Polisi ini diwujudkan bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi PERKESO. Objektif utama PKSB PERKESO ialah seperti berikut:

a) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan, dan kesahihan maklumat serta penyangkalan;

b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;
c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan;
d) Memastikan penyampaian perkhidmatan PERKESO pada tahap keselamatan tertinggi yang dapat meningkatkan keyakinan pihak berkepentingan;
e) Menjamin kelancaran operasi dan kesinambungan perkhidmatan PERKESO dengan meminimumkan impak insiden keselamatan maklumat fizikal dan logikal;
f) Memudahkan perkongsian maklumat yang selamat dan terjamin;
g) Mencegah sebarang penyalahgunaan atau kecurian maklumat PERKESO; dan
h) Menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat dan komunikasi.

1.4 Skop

PKSB PERKESO merupakan panduan utama bagi semua anggota PERKESO serta pihak-pihak yang terlibat dalam pengurusan data atau maklumat di jabatan ini. Polisi ini memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **WAJIB DIBACA, DIFAHAMI**, dan **DIPATUHI** oleh semua anggota PERKESO, termasuk pembekal, pakar runding, pengguna luar serta pihak-pihak berkepentingan yang terlibat dengan perkhidmatan teknologi maklumat dan komunikasi PERKESO. Polisi ini juga terpakai untuk pelindungan terhadap kesemua aset maklumat PERKESO, yang meliputi data dan maklumat dalam bentuk digital (*softcopy*) atau bercetak (*hardcopy*), perkakasan, perisian, infrastruktur ICT, manusia, dan premis. Aset-aset ini adalah sangat penting dan sangat berharga, memastikan PERKESO dapat menjalankan urusan rasmi dengan lancar kepada masyarakat, sektor swasta, serta jabatan kerajaan yang berkaitan. PKSB PERKESO menetapkan keperluan asas seperti yang berikut:

a) **Kebolehcapaian Data dan Maklumat**: Data dan maklumat mesti dapat dicapai secara berterusan dengan pantas, tepat, mudah, dan boleh dipercayai. Ini adalah penting untuk memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b) **Kerahsiaan dan Kesempurnaan Maklumat**: Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dengan baik pada setiap

masa untuk memastikan ketepatan serta melindungi kepentingan kerajaan, perkhidmatan, dan masyarakat.

Untuk memastikan keselamatan aset maklumat sepanjang masa, PKSB PERKESO meliputi perlindungan semua bentuk maklumat kerajaan yang diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan dan dimusnahkan serta diarkibkan dalam persekitaran ICT PERKESO. Perlindungan ini dilaksanakan melalui sistem kawalan dan prosedur pengendalian yang menyeluruh bagi elemen-elemen yang berikut:

a) Data atau Maklumat (*Data or Information*)

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

b) Salinan Digital (*Softcopy*)

Koleksi fakta-fakta dalam digital atau elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif PERKESO (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 PERKESO (Contohnya: Sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, fail-fail dan lain-lain)

d) Perkakasan (*Hardware*)

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan PERKESO, contohnya; komputer, pelayan, storan, peralatan komunikasi dan sebagainya

e) Perisian (*Software*)

Perisian ialah satu set arahan atau program yang diberi kepada komputer untuk melaksanakan tugas-tugas tertentu. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat PERKESO.

f) Aplikasi (*Application*)

Merujuk kepada perisian yang dibangunkan dan digunakan untuk menyokong pelaksanaan fungsi dan proses dalam sesebuah organisasi, sama ada dalam bentuk operasi harian, pentadbiran, pemantauan, atau kawalan keselamatan. Contoh aplikasi sistem seperti sistem perakaunan, sistem pelaburan dan sebagainya.

g) Infrastruktur ICT *(ICT Infrastructure*)

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, pelayan, pangkalan data, rangkaian LAN dan WAN, Internet, sistem komunikasi, pusat data, perkhidmatan pengkomputeran awan (*cloud computing*), peralatan ICT 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 dalam PERKESO.

h) Manusia (*People*)

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

i) Premis (*Premise*)

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

Polisi ini memastikan bahawa setiap aspek di atas diberikan perlindungan yang sewajarnya, meminimumkan risiko dan mengekalkan integriti operasi PERKESO. Setiap

perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai ketidakpatuhan.

2.0 PERNYATAAN POLISI

PERKESO komited untuk mengekalkan persekitaran yang selamat bagi aset maklumat dengan melaksanakan kawalan keselamatan siber yang berkesan selaras dengan standard dan rangka kerja keselamatan siber yang ditetapkan oleh jabatan ini dan NACSA.

2.1 Prinsip Keselamatan Data dan Maklumat

Prinsip-prinsip keselamatan data dan maklumat yang menjadi asas kepada Polisi Keselamatan Siber PERKESO dan perlu dipatuhi ialah seperti yang berikut:

a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017).

b) Hak Akses Minimum

Hak akses kepada pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat atau maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset maklumat PERKESO. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber/ aset maklumat. Untuk

menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka. 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 standard, 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*), PERKESO hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, keselamatan dan aplikasi mengikut kesesuaian.

e) Prinsip Kepercayaan Sifar (*Zero Trust*)

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter rangkaian PERKESO. Setiap permintaan untuk mencapai data atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menyatakan bahawa:

i) semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;

ii) capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik, termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian, serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti, tanpa mengira lokasi fizikal, untuk memastikan keselamatan yang maksimum; dan

iii) menekankan prinsip keistimewaan yang paling sedikit, capaian kepada sumber yang perlu dicapai akan diberikan berdasarkan keperluan, apabila diperlukan dan hanya untuk tempoh masa yang ditetapkan.

f) Pengauditan

Pengauditan merujuk kepada tindakan mengenal pasti insiden keselamatan atau keadaan yang boleh mengancam keselamatan sistem ICT. Semua aset ICT tidak terkecuali komputer, pelayan (*server*), penghala (*router*), tembok api (*firewall*), dan peralatan rangkaian hendaklah berupaya menjana serta menyimpan log tindakan keselamatan atau jejak audit (*audit trail*) bagi tujuan pemantauan, pengesanan dan penyiasatan insiden;

g) Pematuhan

Polisi Keselamatan Siber PERKESO hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat;

h) Pemulihan

Pemulihan adalah untuk memastikan kesediaan dan kebolehcapaian dengan meminimumkan sebarang gangguan atau kerugian yang mungkin timbul akibat ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan/sandaran/replikasi dan mewujudkan pelan pemulihan bencana IT (ITDRP)/ pelan kesinambungan perkhidmatan (BCP); dan

i) Saling Bergantungan

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

3.0 CIRI KESELAMATAN DATA DAN MAKLUMAT

Ciri-ciri keselamatan data dan maklumat yang perlu diberi perhatian oleh semua pihak merangkumi perkara yang berikut:

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, atau penerimaan data atau maklumat tidak boleh menafikan 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 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 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 menyediaan dan pengaktifan pelan pemulihan bencana IT (ITDRP), menyediakan sistem sandaran/replikasi, dan melaksanakan pengurusan risiko yang menyeluruh untuk mengurangkan gangguan terhadap capaian data dan maklumat.

4.0 IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

Ketidakpatuhan terhadap Polisi Keselamatan Siber PERKESO boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

a) Risiko Keselamatan: Ketidakpatuhan boleh menyebabkan pendedahan data sensitif, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

b) Gangguan Operasi: Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Jabatan, termasuk masa henti sistem, kehilangan data, dan

kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

c) **Kesan Undang-Undang:** Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran undang-undang siber.

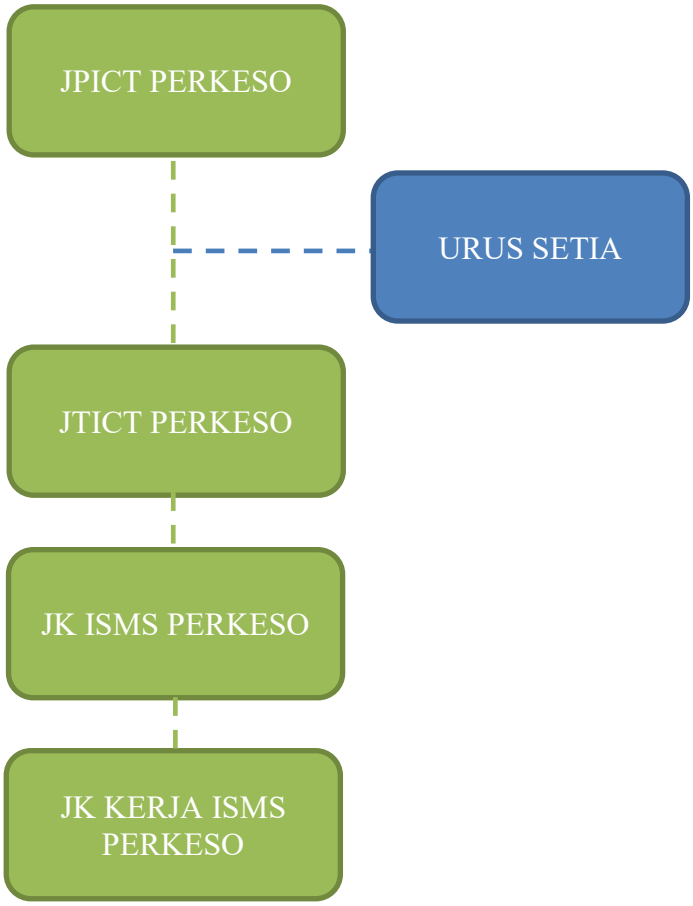
d) **Kerugian Kewangan:** Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan Jabatan.

e) **Kerosakan Reputasi:** Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi PERKESO, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan PERKESO dalam menguruskan keselamatan maklumat.

f) **Tindakan Disiplin**: Semua anggota PERKESO yang didapati tidak mematuhi PKSB ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

5.0 TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKSB PERKESO, sebuah struktur tadbir urus yang mantap telah diwujudkan dengan penubuhan Jawatankuasa Pemandu ICT (JPICT) PERKESO. Struktur Tadbir Urus JPICT PERKESO seperti Rajah 1 di bawah :



RAJAH 1 : Struktur Jawatankuasa Pemandu ICT (JPICT) PERKESO

a) Keahlian Jawatankuasa ini adalah seperti berikut :

Pengerusi : Ketua Pegawai Eksekutif Kumpulan

Ahli :

(i) Timbalan Ketua Eksekutif (Operasi)

(ii) Timbalan Ketua Eksekutif (Strategi dan Korporat)

(iii) Ketua Pegawai Kewangan

(iv) Ketua Pegawai Perundangan

(v) Ketua Bahagian ICT

(vi) Ketua Bahagian Perolehan

(vii) Ketua Cawangan Pengurusan Risiko

(viii) Ketua Cawangan Aplikasi ICT

Urus Setia : Bahagian Strategi dan Transformasi

6.0 PENGURUSAN RISIKO

PERKESO hendaklah mengambil kira kewujudan risiko ke atas aset maklumat akibat dari kelemahan (*vulnerability*) dan ancaman yang semakin meningkat masa kini. Oleh itu, PERKESO hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset maklumat supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan yang optimum. PERKESO hendaklah melaksanakan penilaian risiko keselamatan maklumat secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan maklumat. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan penemuan penilaian risiko.

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

PERKESO bertanggungjawab melaksanakan dan menguruskan risiko keselamatan maklumat selaras dengan keperluan Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam, Akta Keselamatan Siber 2024 dan Tataamalan Bagi NCII Yang Ditetapkan Oleh JDN. PERKESO hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

i) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
ii) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan PERKESO;
iii) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
iv) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding, pengguna luar dan pihak lain yang berkepentingan

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** oleh BAR dan dimaklumkan kepada Pemilik Perkhidmatan atau Mesyuarat Jawatankuasa ISMS PERKESO.

7.0 PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Setiap projek di PERKESO hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKSB PERKESO, Tataamalan Bagi NCII Yang Ditetapkan Oleh JDN dan surat pekeliling/arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan (*Data in Use*), data-dalam-pergerakan (*Data in Transit*), data-dalam-simpanan (*Data at Rest*) 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 eribadi 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

Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti switch, penghala rangkaian, tembok keselamatan, peranti *load balancer,* peranti *Virtual Private Network* (VPN) dan kabel. 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

Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi dan sistem operasi. 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.

d) Pelayan

Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat. 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

Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT. Cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat hendaklah dirujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) untuk mendapatkan khidmat nasihat serta hendaklah selaras dengan perundangan dan arahan yang sedang berkuat kuasa. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan *defend-in-depth*. 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.

8.0 KAWALAN ORGANISASI

8.1 Polisi Keselamatan Siber

Objektif :

Memastikan polisi keselamatan siber bersesuaian, berterusan dan seiring dengan hala tuju pengurusan dalam menyokong keselamatan maklumat selari dengan fungsi PERKESO, undang-undang yang berkuat kuasa dan keperluan kontrak dan/atau perjanjian.

DP8.1.1 Pelaksanaan Polisi

Hanya terpakai untuk anggota PERKESO sahaja

DP8.1.2 Pengesahan Polisi

Hanya terpakai untuk anggota PERKESO sahaja

DP8.1.3 Penguatkuasaan Polisi

PKSB PERKESO mestilah dipatuhi oleh semua pengguna luar yang berurusan dengan perkhidmatan ICT di PERKESO. Setiap pengguna luar dan pihak yang berurusan dengan perkhidmatan ICT di PERKESO hendaklah menandatangani Borang Perjanjian Kerahsiaan – NDA PERKESO (Lampiran B), Borang Tapisan Keselamatan – KPKK 11 dan Akuan Pematuhan PKSB PERKESO. Sebarang ketidakpatuhan kepada dasar ini boleh mengakibatkan tindakan diambil terhadap anggota termasuklah tindakan tatatertib termasuk sebarang remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang berkuat	Pengguna Luar

kuasa. Piawaian dan prosedur yang berkaitan hendaklah dipatuhi.	
DP8.1.4 Penyebaran Polisi	
Program kesedaran tentang polisi ini hendaklah diatur dan diselaraskan mengikut keperluan.	Pengguna Luar
DP8.1.5 Pengecualian Polisi	
PKSB PERKESO adalah terpakai kepada semua pengguna luar dan tiada pengecualian diberikan.	Pengguna Luar
DP8.1.6 Penyelenggaraan Polisi	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.1.7 Kajian Semula/Semakan Polisi	
Hanya terpakai untuk anggota PERKESO sahaja	
8.2 Peranan dan Tanggungjawab Keselamatan Maklumat	
Objektif: Mewujudkan struktur, peranan dan tanggungjawab dalam pengurusan keselamatan maklumat di PERKESO.	
DP8.2.1 Ketua Pegawai Eksekutif Kumpulan (KPEK)	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.2.2 Timbalan Ketua Eksekutif Strategi dan Korporat (TKESK)	
Hanya terpakai untuk anggota PERKESO sahaja	

DP8.2.3 Ketua Pegawai Digital (CDO)
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.4 Pengurus ICT
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.4 Pegawai Keselamatan ICT (ICTSO)
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.5 Ketua Pegawai / Ketua Bahagian / Ketua Cawangan
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.6 Jawatankuasa Pemandu ICT (JPICT) PERKESO
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.7 Jawatankuasa Teknikal ICT (JTICT) PERKESO
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.8 *Cyber Security Incident Response Team* (CSIRT) PERKESO
Hanya terpakai untuk anggota PERKESO sahaja
DP8.2.9 Pasukan Petugas Keselamatan Siber (PPKS) PERKESO
Hanya terpakai untuk anggota PERKESO sahaja

8.3 Pengasingan Tugas

Objektif:
Menerangkan perbezaan tugas setiap individu dengan lebih jelas dan teratur untuk mencegah daripada berlakunya kebocoran serta kesilapan.

DP8.3.1 Koordinator Pasukan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

DP8.3.2 Pemilik Sistem / Pemilik Maklumat / Pengurus Projek / *Change Management*

Hanya terpakai untuk anggota PERKESO sahaja

DP8.3.3 Pegawai Aset

Hanya terpakai untuk anggota PERKESO sahaja

DP8.3.4 Anggota PERKESO

Hanya terpakai untuk anggota PERKESO sahaja

DP8.3.5 Pengguna Luar

Peranan dan tanggungjawab pengguna luar adalah seperti berikut: a) Membaca, memahami dan mematuhi Polisi ini; b) Mengetahui dan memahami implikasi keselamatan maklumat dan keselamatan siber akibat daripada tindakannya ; c) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat PERKESO;	Pengguna Luar

d) Melaksanakan langkah-langkah perlindungan seperti berikut :
   (i) Menghalang pendedahan maklumat kepada pihak yang tidak berkaitan;
   (ii) Menjaga kerahsiaan kata laluan yang diberikan;
   (iii) Menjaga tahap kerahsiaan maklumat;
   (iv) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, pengemaskinian, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
   (v) Menjaga kerahsiaan kawalan keselamatan maklumat dari diketahui umum.

e) Menggunakan kemudahan ICT dengan berpandukan garis panduan yang telah ditetapkan; dan

f) Menandatangani **Surat Akuan Pematuhan PKSB PERKESO, Borang *Non Disclosure Agreement* (NDA)** dan **Borang Tapisan Keselamatan (KPKK 11-CGSO).**

8.4 Tanggungjawab Pengurusan

Objektif:

Memastikan pihak pengurusan dan anggota PERKESO memahami peranan serta memenuhi tanggungjawab dalam keselamatan maklumat.

DP8.4.1 Tanggungjawab Pengurusan

Hanya terpakai untuk anggota PERKESO sahaja

8.5 Hubungan dengan Pihak Berkuasa

Objektif:

PERKESO hendaklah mewujudkan dan mengekalkan hubungan baik dengan pihak berkuasa yang berkaitan.

DP8.5.1 Hubungan dengan Pihak Berkuasa

Hanya terpakai untuk anggota PERKESO sahaja

8.6 Hubungan Dengan Kumpulan Berkepentingan

Objektif:
Memastikan maklumat yang diperlukan oleh pihak berkepentingan dengan PERKESO disediakan.

DP8.6.1 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus

Hanya terpakai untuk anggota PERKESO sahaja

DP8.7 Perisikan Ancaman

Objektif:
Memastikan kawalan ancaman keselamatan terhadap PERKESO difahami, di analisa dan kaedah tindakan yang bersesuaian dilaksanakan.

DP8.7.1 Pengumpulan Maklumat Ancaman

Hanya terpakai untuk anggota PERKESO sahaja

DP8.7.2 Analisa Maklumat Ancaman

Hanya terpakai untuk anggota PERKESO sahaja

DP8.7.3 Tindakan ke Atas Maklumat Ancaman

Hanya terpakai untuk anggota PERKESO sahaja

8.8 Keselamatan Maklumat dalam Pengurusan Projek

Objektif:

Memastikan keselamatan maklumat diambil kira dalam pengurusan projek.

DP8.8.1 Keselamatan Maklumat Dalam Pengurusan Projek

Hanya terpakai untuk anggota PERKESO, pembekal dan pakar runding sahaja

DP8.8.2 Analisis dan Spesifikasi Keperluan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.9 Maklumat Inventori dan Aset

Objektif:

Memastikan pengurusan maklumat dan aset dikenal pasti, dikelaskan, direkodkan, diselenggarakan dan penempatan ditetapkan untuk perlindungan keselamatan.

DP8.9.1 Inventori dan Penempatan Maklumat Serta Aset ICT

Hanya terpakai untuk anggota PERKESO sahaja

DP8.9.2 Tanggungjawab Pemilik

Hanya terpakai untuk anggota PERKESO sahaja

DP8.9.3 Pengelasan Maklumat Aset

Hanya terpakai untuk anggota PERKESO Sahaja

8.10 Penggunaan Maklumat dan Aset Yang Diterima

Objektif:

Memastikan setiap maklumat dan Aset ICT yang berkaitan dilindungi, digunakan dan dikendalikan dengan sewajarnya.

DP8.10.1 Penggunaan Maklumat dan Aset

Memastikan penggunaan aset untuk tujuan rasmi dan mengikut fungsi sebenar yang telah ditetapkan oleh PERKESO. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan pengguna luar yang mempunyai capaian ke atas maklumat dan Aset ICT hendaklah bertanggungjawab terhadap keperluan perlindungan serta pengendalian keselamatan maklumat; b) Melindungi maklumat dan aset PERKESO berkaitan daripada ancaman yang berasal dari dalam atau luar PERKESO; c) Menyediakan prosedur pengurusan pengendalian maklumat yang merangkumi penggunaan, kebenaran, perkongsian dan pemantauan maklumat; d) Memastikan kawalan capaian yang dibenarkan mengikut tahap klasifikasi pengelasan maklumat; e) Menyelenggarakan rekod berkaitan senarai pengguna yang dibenarkan untuk capaian maklumat; f) Memastikan kawalan ke atas salinan maklumat, storan maklumat dan perlu melaksanakan pelabelan media storan dengan jelas; dan g) Memperoleh kebenaran untuk melaksanakan pelupusan maklumat dan aset berdasarkan kaedah yang bersesuaian.	Pengguna Luar

DP8.10.2 Pengendalian Maklumat dan Aset ICT

Hanya terpakai untuk anggota PERKESO sahaja

8.11 Pemulangan Aset

Objektif:

Memastikan proses pemulangan aset dilaksanakan apabila berlaku perubahan dan penamatan perkhidmatan, kontrak atau perjanjian.

DP8.11.1 Pemulangan Aset

Hanya terpakai untuk anggota PERKESO sahaja

8.12 Klasifikasi Maklumat

Objektif:

Memastikan pengenalpastian dan pemahaman tentang keperluan perlindungan maklumat mengikut kepentingan di PERKESO.

DP8.12.1 Pengelasan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.13 Pelabelan Maklumat

Objektif:

Memastikan pelabelan maklumat dilaksanakan bagi memudahkan pengurusan penyimpanan maklumat.

DP8.13.1 Pelabelan Maklumat

Hanya terpakai untuk anggota PERKESO Sahaja

8.14 Pemindahan Maklumat

Objektif:

Memastikan keselamatan semasa pemindahan maklumat kepada pihak ketiga atau sebaliknya. Pemindahan maklumat secara dalaman atau luaran hendaklah mengikut syarat atau perjanjian yang ditetapkan.

DP8.14.1 Prosedur Pemindahan Maklumat

Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara PERKESO dan pengguna luar terjamin. Perkara yang hendaklah dipatuhi adalah seperti berikut: a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b) Terma pemindahan data, maklumat dan perisian antara PERKESO dengan pengguna luar hendaklah dimasukkan di dalam Perjanjian; c) Media yang mengandungi maklumat hendaklah dilindungi; d) Memastikan maklumat yang terdapat dalam E-mel elektronik hendaklah dilindungi sebaik-baiknya; e) Kawalan ke atas pemindahan maklumat daripada dicerobohi, diubah, disalin, dimusnahkan dan sebagainya; f) Pemindahan maklumat hendaklah direkodkan bagi kawalan pengesanan; g) Memastikan kakitangan yang dibenarkan sahaja bertanggungjawab semasa pemindahan maklumat; h) Mengenal pasti pegawai yang bertanggungjawab sekiranya berlaku insiden keselamatan;	Pengguna Luar

i) Memastikan kawalan keselamatan dilaksanakan berdasarkan peringkat pengelasan maklumat; j) Ketersediaan dan boleh dipercayai bagi perkhidmatan pemindahan maklumat yang digunakan; k) Mematuhi peraturan dan pekeliling semasa yang masih berkuat kuasa berkaitan pemusnahan maklumat; l) Pematuhan kepada mana-mana undang-undang/ peraturan/ pekeliling yang berkaitan dengan pemindahan data; m) Mengehadkan pemindahan maklumat untuk tujuan rasmi dan yang dibenarkan sahaja; dan n) Mewujudkan *Non-Disclosure Agreements* (NDA) bagi memastikan kerahsiaan, integriti dan ketersediaan (CIA) maklumat terpelihara semasa proses pemindahan maklumat.	
DP8.14.2 Perjanjian Mengenai Pemindahan Maklumat	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.14.3 Pemindahan Elektronik	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.14.4 Pesanan Elektronik	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.14.5 Pemindahan Storan Fizikal	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.14.6 Pemindahan Lisan	

Hanya terpakai untuk anggota PERKESO sahaja

8.15 Kawalan Capaian

Objektif:

Memastikan akses bagi menghalang capaian yang tidak dibenarkan kepada maklumat dan lain-lain yang berkaitan aset .

DP8.15.1 Keperluan Kawalan Capaian

Hanya terpakai untuk anggota PERKESO sahaja

DP8.15.2 Pelaksanaan Peraturan Kawalan Akses

Hanya terpakai untuk anggota PERKESO sahaja

DP8.15.3 Prinsip Kawalan Capaian

Hanya terpakai untuk anggota PERKESO sahaja

5.16 Pengurusan Identiti

Objektif:

Memastikan ID pengguna adalah unik dan sesuai ke atas entiti untuk mengakses sistem dan aset PERKESO lain yang berkaitan.

DP8.16.1 Proses Pengurusan Identiti

Hanya terpakai untuk anggota PERKESO sahaja

DP8.16.2 Prosedur Penyediaan atau Pembatalan Capaian

Hanya terpakai untuk anggota PERKESO sahaja

8.17 Pengesahan Maklumat

Objektif:
Memastikan pengesahan entiti yang betul untuk mengelakkan kegagalan capaian maklumat.

DP8.17.1 Proses Pengesahan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

DP8.17.2 Sistem Pengurusan Kata Laluan

Hanya terpakai untuk anggota PERKESO sahaja

8.18 Hak Capaian

Objektif:
Memastikan hak capaian kepada maklumat dan aset lain dibenarkan mengikut keperluan.

DP8.18.1 Peruntukan dan Pembatalan Hak Capaian

Hanya terpakai untuk anggota PERKESO sahaja

DP8.18.2 Kajian Semula Hak Capaian

Hanya terpakai untuk anggota PERKESO sahaja

DP8.18.3 Pembatalan atau Pelarasan Hak Capaian

Hanya terpakai untuk anggota PERKESO sahaja

DP8.18.4 Tanggungjawab Pengguna

Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan identiti mereka.	Pengguna Luar

8.19 Keselamatan Maklumat Dengan Pihak

Objektif:
Memastikan semua pihak ketiga adalah tertakluk kepada peraturan yang berkuat kuasa.

DP8.19.1 Polisi Keselamatan Siber Ke Atas Pengguna Luar

Keselamatan maklumat ke atas pengguna luar hendaklah mematuhi perkara seperti berikut: a) Mengenal pasti dan merekodkan pengguna luar yang terlibat dengan aspek kerahsiaan, integriti dan ketersediaan maklumat PERKESO; b) Mewujudkan kaedah penilaian dan pemilihan pengguna luar berdasarkan klasifikasi maklumat, produk dan perkhidmatan; c) Menilai dan memilih produk atau perkhidmatan pengguna luar yang mempunyai kawalan keselamatan maklumat serta melaksanakan semakan berkala bagi memastikan integriti dan keselamatan maklumat terjamin; d) Mengenal pasti maklumat PERKESO, perkhidmatan ICT dan infrastruktur fizikal yang boleh diakses, dipantau, dikawal atau digunakan oleh pengguna luar; e) Mengenal pasti jenis komponen dan perkhidmatan infrastruktur ICT yang disediakan oleh pengguna luar yang boleh menjejaskan kerahsiaan, integriti dan ketersediaan maklumat PERKESO; f) Menilai dan mengurus risiko keselamatan maklumat yang berkaitan dengan:	Pemilik Projek, Pengguna Luar

i. Penggunaan maklumat dan aset pengguna luar;
ii. Kerosakan (*malfunction*) atau kelemahan produk (termasuk komponen perisian dan sub-komponen); atau
iii. Perkhidmatan yang disediakan oleh pengguna luar;

g) Memantau pematuhan dan keperluan keselamatan maklumat yang ditetapkan kepada semua pengguna luar;

h) Mencegah ketidakpatuhan pengguna luar, sama ada dikesan melalui pemantauan atau sumber lain;

i) Pengurusan insiden berkaitan produk atau perkhidmatan di bawah tanggungjawab PERKESO dan pengguna luar;

j) Keupayaan tindakan pemulihan dan pelan kontingensi (*contingency plan*) untuk memastikan ketersediaan maklumat;

k) Program kesedaran dan latihan kepada kakitangan PERKESO yang melibatkan pengguna luar termasuk mempunyai akses kepada maklumat;

l) Memastikan keselamatan maklumat sentiasa terjaga sepanjang tempoh pemindahan maklumat atau aset lain yang berkaitan;

m) Memastikan keselamatan maklumat semasa penamatan perkhidmatan pengguna luar merangkumi perkara berikut:
i. Pembatalan hak akses;
ii. Pengendalian maklumat;
iii. Menentukan pemilikan harta intelek;
iv. Pemindahan maklumat sekiranya berlaku pertukaran pengguna luar;
v. Pengurusan rekod;
vi. Pemulangan aset;
vii. Pelupusan maklumat dan aset lain berkaitan secara selamat; dan
viii. Keperluan kerahsiaan yang berterusan.

n) Tahap keselamatan kakitangan dan keselamatan fizikal yang perlu dipatuhi pengguna luar dengan mematuhi keperluan berikut: i. Borang Akuan Pematuhan Polisi Keselamatan Siber (PKSB) PERKESO; ii. Borang Perjanjian Kerahsiaan (NDA - PERKESO); dan iii. Borang Tapisan Keselamatan Kasar (KPKK 11 - CGSO).	

8.20 Keselamatan Maklumat Dalam Perjanjian Pihak Ketiga

Objektif:
Memastikan keselamatan maklumat dengan pihak ketiga melalui perjanjian yang telah dipersetujui.

DP8.20.1 Kawalan Keselamatan Maklumat Melalui Penjanjian Dengan Pengguna Luar

Bahagian ICT / Bahagian yang berkaitan hendaklah mentakrifkan, menyediakan dan mempersetujui semua keperluan keselamatan maklumat yang berkaitan dengan pengguna luar yang boleh mengakses, memproses, menggunakan, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat PERKESO untuk disemak oleh Bahagian Perundangan dan Pendakwaan. Klausa perjanjian hendaklah memperuntukkan tanggungjawab pengguna luar bagi memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak PERKESO selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.	Pengguna Luar

Sekiranya pengguna luar gagal mematuhi peraturan kawalan keselamatan tersebut, pihak PERKESO mempunyai kuasa untuk menghalang pengguna luar daripada melaksanakan perkhidmatan tersebut dan boleh menamatkan apa-apa perjanjian dengan pengguna luar tersebut, sekiranya masih berkuat kuasa. Selain itu, perjanjian juga perlu memperuntukkan bahawa pengguna luar hendaklah membayar ganti rugi kepada PERKESO sekiranya berlaku apa-apa pelanggaran peraturan kawalan keselamatan maklumat dan infrastruktur ICT PERKESO. Dalam pemilihan pengguna luar, perkara yang hendaklah dipatuhi adalah tertakluk kepada semua perkara teknikal dan komersial yang telah dipersetujui oleh Bahagian yang berkaitan:

a) PERKESO digalakkan memilih pengguna luar yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;
b) Pengguna Luar yang mempunyai pensijilan keselamatan berkaitan keselamatan maklumat dan keselamatan siber yang berkaitan hendaklah diberi keutamaan;
c) Semua wakil pengguna luar hendaklah mempunyai kelulusan keselamatan berkaitan keselamatan maklumat dan keselamatan siber daripada jabatan berkaitan;
d) Produk atau perkhidmatan yang ditawarkan oleh pengguna luar hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;
e) Jawatankuasa boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pengguna luar melalui laporan yang dikemukakan oleh pengguna luar;
f) Pengguna Luar hendaklah mempunyai pelan pengurusan risiko yang sempurna bagi mencegah risiko serangan siber ke atas sistem, laman web atau aplikasi terutamanya dalam menjamin keselamatan data serta pelan

perancangan *recovery* atau *damage control* sekiranya berlaku serangan siber.

g) **Pengguna Luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menggunakan, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan PERKESO dan *Non Disclosure Agreement* (NDA) PERKESO di Lampiran B**;

h) Pengguna Luar hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh PERKESO;

i) Pengguna Luar hendaklah menyediakan latihan dan program kesedaran untuk topik khusus keselamatan maklumat;

j) Pengguna Luar hendaklah mengadakan keperluan dan menyediakan prosedur pengurusan insiden keselamatan;

k) Pengguna Luar hendaklah membayar ganti rugi dan mengambil langkah pemulihan yang sewajarnya bagi kegagalan pematuhan kontrak oleh pengguna luar;

l) Laporan jaminan pengesahan keselamatan maklumat dan pembuktian oleh pengguna luar;

m) Penyelesaian ketidakpatuhan dan proses penyelesaian konflik;

n) Menyediakan sandaran (*backup*) berdasarkan keperluan PERKESO dari segi kekerapan, jenis dan lokasi penyimpanan;

o) Memastikan ketersediaan tapak alternatif pemulihan bencana sekiranya tapak utama gagal berfungsi;

p) Menyediakan proses pengurusan perubahan;

q) Menyediakan kawalan keselamatan fizikal yang selari dengan tahap klasifikasi maklumat;

r) Menyedia kawalan pemindahan terhadap maklumat fizikal atau logikal;

s) Mematuhi klausa penamatan selepas perjanjian yang merangkumi pengurusan rekod, pemulangan aset,

pelupusan maklumat dan aset lain yang berkaitan secara selamat berdasarkan pematuhan kerahsiaan semasa; t) Maklumat yang disimpan oleh pengguna luar hendaklah dihapus dengan selamat jika tidak lagi diperlukan; dan u) Memastikan penyerahan dokumen dilaksanakan kepada PERKESO atau pihak lain sebelum kontrak tamat.	

8.21 Pengurusan Keselamatan Maklumat Dalam Rantaian Maklumat Dan Komunikasi ICT

Objektif:

Memastikan persetujuan kawalan keselamatan bersama pihak ketiga dimeterai.

DP8.21.1 Kawalan Rantaian Bekalan Maklumat dan Komunikasi

Perjanjian dengan pengguna luar hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira ialah seperti yang berikut : a) Menentukan keperluan berkaitan keselamatan maklumat untuk kegunaan perolehan bekalan dan perkhidmatan; b) Pengguna Luar utama hendaklah memastikan risiko keselamatan maklumat berkaitan dengan produk ICT dan rantaian pembekalan produk ditangani; c) Memastikan jaminan daripada pengguna luar bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; d) Pengguna Luar utama hendaklah menghebahkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan;	Pengguna Luar

e) Pengguna Luar utama hendaklah menghebahkan keperluan keselamatan maklumat berkaitan dengan produk ICT kepada pengguna luar yang lain;
f) Melaksanakan satu proses/kaedah pemantauan yang boleh mengesahkan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat PERKESO;
g) Mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan;
h) Memastikan jaminan dari pengguna luar bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik;
i) Memastikan komponen produk yang dibekalkan adalah tulen dan tidak diubah dari spesifikasi asal atau mengikut keperluan PERKESO;
j) Memastikan bahawa produk ICT memenuhi standard keselamatan yang ditetapkan atau melalui proses pensijilan rasmi atau amalan terbaik;
k) Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara PERKESO dan pengguna luar; dan
l) Memastikan pengurusan kitaran hayat dan ketersediaan komponen ICT yang tidak lagi tersedia disebabkan pengguna luar tidak lagi beroperasi atau pengguna luar tidak lagi menyediakan komponen ini disebabkan kemajuan teknologi. Ini bagi mengurangkan impak risiko keselamatan ke atas PERKESO.

8.22 Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pihak Ketiga

Objektif:

Memastikan pemantauan, penilaian dan pengurusan perubahan dilaksanakan ke atas pihak ketiga.

DP8.22.1 Pemantauan dan Penilaian Perkhidmatan Pengguna Luar	
PERKESO hendaklah memantau, menyemak, menilai, dan mengurus perubahan dalam amalan keselamatan maklumat pengguna luar dan penyedia perkhidmatan secara berterusan. PERKESO hendaklah sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pengguna luar secara berkala dan mengurus perubahan dalam amalan risiko keselamatan maklumat pengguna luar dan penyedia perkhidmatan. Perkara-perkara yang hendaklah diambil kira adalah seperti yang berikut: a) Memastikan tahap pencapaian perkhidmatan pengguna luar selaras dengan kontrak dan/atau perjanjian; b) Laporan perkhidmatan yang dihasilkan oleh pengguna luar hendaklah dipantau dan status kemajuan dikemukakan kepada PERKESO; c) Memaklumkan mengenai insiden keselamatan kepada pengguna luar dan mengkaji maklumat seperti yang dikehendaki dalam kontrak dan/atau perjanjian; d) Mengambil tindakan terhadap sebarang insiden keselamatan maklumat yang dikenal pasti; e) Menguruskan kelemahan keselamatan maklumat yang dikenal pasti; dan f) Pengguna Luar yang didapati tidak memenuhi keperluan kontrak dan/atau perjanjian boleh dikenakan tindakan bersesuaian seperti penalti.	Pengguna Luar

DP8.22.2 Pengurusan Perubahan Kepada Perkhidmatan Pengguna Luar	
Perubahan kepada peruntukan perkhidmatan oleh pengguna luar, termasuk mempertahan dan menambah	Pengguna Luar

baik polisi keselamatan siber sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses yang terlibat dan penilaian semula risiko.

Setiap perubahan perkhidmatan pengguna luar hendaklah dilaksanakan secara teratur dan mengikut *Standard Operating Procedure* (SOP) yang ditetapkan. Perkara yang perlu diambil kira adalah seperti berikut:

a) Memastikan perubahan dalam perkhidmatan pengguna luar dipersetujui bersama dan menguntungkan bagi pihak kerajaan;
b) Memastikan perubahan dalam perjanjian dengan pengguna luar mengambil kira maklumat kritikal PERKESO, sistem serta proses yang terlibat dan kajian risiko;
c) Pemantauan dan persetujuan ke atas perubahan perkhidmatan pengguna luar yang merangkumi perkara berikut:
    i. Peningkatan kepada perkhidmatan/produk sedia ada termasuk rangkaian, perisian, versi dan alatan pembangunan;
    ii. Pembangunan sebarang aplikasi dan sistem baharu;
    iii. Pengubahsuaian atau kemas kini polisi dan prosedur pengguna luar;
    iv. Kaedah kawalan baharu atau yang dikemas kini bagi menyelesaikan insiden keselamatan maklumat dan meningkatkan keselamatan maklumat; dan
    v. Perubahan lokasi perkhidmatan dan subkontraktor.

8.23 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Pengkomputeran Awan

Objektif:

Memastikan pengurusan keselamatan maklumat bagi pengkomputeran awam.

DP8.23.1 Keselamatan Maklumat Untuk Perkhidmatan Pengkomputeran Awan

Perkara yang perlu dipatuhi adalah seperti berikut : a) Memastikan pematuhan pengguna luar dan pengguna terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak berkaitan dengan perkhidmatan pengkomputeran awan serta arahan pihak berkuasa Kerajaan seperti Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan Kementerian Digital Malaysia yang berkuat kuasa serta pengurusan perkhidmatan yang disediakan oleh pengguna luar seperti di DP5.21 dan DP5.22 (Bidang PKSB PERKESO); b) Menentu/mentakrif dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; c) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; d) Melaksanakan kawalan terhadap keperluan langganan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan; e) Mengenal pasti klasifikasi maklumat atau data dalam penggunaan perkhidmatan pengkomputeran awan; f) Mengenal pasti ciri-ciri asas dan model perkhidmatan pengkomputeran awan yang hendak digunakan; g) Menetapkan tugas dan tanggungjawab ke atas pengurusan perkhidmatan awan; h) Menentukan tanggungjawab kawalan keselamatan perkhidmatan awan di antara penyedia dan pengguna perkhidmatan awan;	Pengguna Luar

i) Memastikan kemampuan dan jaminan kawalan keselamatan maklumat yang dilaksanakan oleh penyedia perkhidmatan awan; j) Struktur tadbir urus hendaklah dikenal pasti berdasarkan peranan dan tanggungjawab untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat dalam pengurusan pengkomputeran awan; k) Pematuhan pengurusan maklumat rahsia rasmi dalam persekitaran ICT menjadi prasyarat (*prerequisite*) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan; l) Memastikan pengurusan kontrak dan terma keselamatan dalam penggunaan perkhidmatan pengkomputeran awan; m) Memastikan perlindungan migrasi data ke pengkomputeran awan, perlindungan data semasa penghantaran dan perlindungan data dalam simpanan logikal atau fizikal oleh pihak penyedia perkhidmatan; n) Memantau, menyemak dan menilai keselamatan maklumat dalam perkhidmatan pengkomputeran awan; o) Memastikan pengurusan insiden oleh penyedia perkhidmatan pengkomputeran awan; p) Memastikan penyedia perkhidmatan mewujudkan atau mempunyai pelan pengurusan kesinambungan perkhidmatan (PKP); dan q) Memastikan penamatan perkhidmatan pengkomputeran awan dilaksanakan mengikut peraturan berkuat kuasa.	
DP8.23.2 Pengurusan Kontrak Perkhidmatan Awan	
Perjanjian dengan penyedia perkhidmatan awan perlu mengandungi perkara berikut:	Pembekal

a) Menyediakan cadangan penggunaan berdasarkan piawaian yang bersesuaian; b) Menguruskan kawalan akses ke perkhidmatan pengkomputeran awan berdasarkan keperluan PERKESO; c) Melaksanakan pemantauan ke atas perisian hasad serta cadangan perlindungan; d) Memproses dan menyimpan maklumat rahsia rasmi PERKESO yang diluluskan sahaja; e) Memberikan khidmat sokongan sekiranya berlaku insiden keselamatan maklumat; f) Memastikan keperluan keselamatan maklumat dipenuhi sekiranya perkhidmatan pengkomputeran awan dilaksanakan oleh pengguna luar; g) Membantu PERKESO mengumpul bukti digital sekiranya diperlukan oleh undang-undang; h) Menyediakan khidmat sokongan yang bersesuaian sekiranya perkhidmatan awan tidak disambung guna; i) Menyediakan sandaran ke atas maklumat dan tetapan konfigurasi perkhidmatan awan; dan j) Menyediakan dan mengembalikan maklumat seperti fail konfigurasi, kod sumber dan maklumat PERKESO sekiranya perkhidmatan pengkomputeran awan ditamatkan.	

DP8.23.3 Pengurusan Perubahan Perkhidmatan Pengkomputeran Awan

Pengurusan perubahan perlu dilaksanakan berdasarkan perkara berikut: a) Pertukaran infrastruktur yang mengubah perkhidmatan yang ditawarkan dalam pengkomputeran awan; b) Penyimpanan atau pemprosesan maklumat mengikut pemetaan geografi yang baharu mengikut undang-undang; dan c) Penyedia melantik syarikat lain sebagai pengendali perkhidmatan pengkomputeran awan.	Pengguna Luar

8.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat

Objektif:

Memastikan perancangan pengurusan insiden keselamatan maklumat yang dilaksanakan adalah konsisten dan teratur.

DP8.24.1 Tanggungjawab dan Prosedur

Hanya terpakai untuk anggota PERKESO sahaja

DP8.24.2 Perancangan dan Persediaan Pengurusan Insiden Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.25 Penilaian dan Tindakan Insiden Keselamatan Maklumat

Objektif:

Mengenal pasti kategori dan penilaian berasaskan keutamaan ke atas semua insiden keselamatan maklumat.

DP8.25.1 Penilaian dan Tindakan Mengenai Insiden Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Objektif:

Melaksanakan tindak balas yang cepat dan berkesan terhadap insiden keselamatan maklumat.

DP5.26.1 Tindak Balas Terhadap Insiden Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.27 Pembelajaran Daripada Insiden Keselamatan Maklumat

Objektif:

Meningkatkan kawalan keselamatan berdasarkan analisa dan penyelesaian insiden keselamatan maklumat yang telah dilaksanakan bagi mengelakkan insiden yang sama berulang.

DP8.27.1 Penambahbaikan Kawalan Daripada Insiden Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.28 Pengumpulan Bahan Bukti

Objektif:

Memastikan pengurusan penyimpanan bukti direkodkan secara konsisten bagi insiden keselamatan maklumat untuk tindakan tatatertib dan undang-undang.

DP8.28.1 Pengumpulan dan Pengendalian Bahan Bukti

Hanya terpakai untuk anggota PERKESO sahaja

8.29 Keselamatan Maklumat Semasa Gangguan

Objektif:

PERKESO hendaklah merancang bagaimana untuk mengekalkan keselamatan maklumat pada tahap yang sesuai semasa gangguan.

DP8.29.1 Keselamatan Maklumat Semasa Gangguan

Hanya terpakai untuk anggota PERKESO sahaja

DP8.29.2 Perancangan Keselamatan Maklumat dalam Kesinambungan Perkhidmatan

Hanya terpakai untuk anggota PERKESO sahaja

DP8.29.3 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Hanya terpakai untuk anggota PERKESO sahaja

DP8.29.4 Mengkaji, Menilai dan Mengesahkan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan

Hanya terpakai untuk anggota PERKESO sahaja

8.30 Ketersediaan ICT Bagi Kesinambungan Perkhidmatan

Objektif:

Memastikan ketersediaan maklumat dan Aset ICT yang berkaitan semasa gangguan berdasarkan Pelan Pemulihan Bencana (DRP).

DP8.30.1 Pengenalpastian Ketersediaan Aset ICT Semasa Gangguan

Hanya terpakai untuk anggota PERKESO sahaja

DP8.30.2 Perancangan Kesinambungan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

DP8.30.3 Pelaksanaan Kesinambungan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

DP8.30.4 Menentusah, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

8.31 Keperluan Undang-Undang, Statutori, Pengawalseliaan dan Kontraktual

Objektif:
Memastikan pematuhan kepada keperluan undang-undang yang berkaitan dengan keselamatan maklumat. Semua keperluan undang-undang, peraturan dan kontrak dan/atau perjanjian yang berkaitan dengan PERKESO perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat.

DP8.31.1 Pematuhan Terhadap Keperluan Undang-Undang dan Kontrak dan/atau Perjanjian

Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak dan/atau perjanjian yang berkaitan dengan keselamatan maklumat dengan menyediakan *Non-Disclosure Agreement* (NDA) mengikut keperluan projek dan menguatkuasakan Perakuan Akta Rahsia Rasmi 1972 (Akta 88). Klausa keselamatan siber adalah sebagaimana dalam **Lampiran C** yang perlu dimasukkan dalam kontrak dan/atau perjanjian dan boleh dipinda, mengikut kesesuaian. Memastikan terma dalam mana-mana kontrak dan/atau perjanjian berkaitan dengan "kerahsiaan" hendaklah memperuntukkan bahawa tanggungjawab kerahsiaan hendaklah terus mengikat kedua-dua pihak walaupun kontrak dan/atau perjanjian telah ditamatkan ("terminated")	Pengguna Luar

atau berakhir ("expired"). Klausa "kerahsiaan" adalah sebagaimana dalam **Lampiran D** yang perlu dimasukkan dalam kontrak dan boleh dipinda, mengikut kesesuaian.	

DP8.31.2 Pengenalpastian Keperluan Perundangan dan Kontrak Yang Terpakai

Bahagian ICT hendaklah mengadakan dokumen pematuhan berdasarkan PKSB yang mengandungi keperluan perundangan, peraturan dan kontrak dan/atau perjanjian hendaklah dikenal pasti dan dipatuhi oleh semua anggota PERKESO dan pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua semua anggota PERKESO dan pengguna luar seperti di **LAMPIRAN E** Pengguna Luar yang melanggar mana-mana klausa dalam *integrity pact* boleh ditamatkan perkhidmatannya.	Pengguna Luar

DP8.31.3 Kawalan Kriptografi

Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi kriptografi; b) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi; c) Sekatan ke atas penggunaan enkripsi; d) Kaedah akses oleh pihak berkuasa Malaysia mengenai maklumat enkripsi perkakasan dan perisian	Pengguna Luar

e) Kesahihan tandatangan digital, meterai dan sijil.	

8.32 Hak Harta Intelek

Objektif:

Bagi memastikan pematuhan ke atas undang-undang terhadap harta intelek.

DP8.32.1 Hak Harta Intelek

Bahagian ICT / Bahagian yang berkaitan hendaklah memastikan kepatuhan terhadap keperluan perundangan, peraturan dan kontrak dan/atau perjanjian yang berkaitan dengan 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. Pengguna Luar perlu mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. PERKESO hendaklah mematuhi: a) Keperluan hak cipta yang berkaitan dengan bahan *proprietary*, perisian, dan reka bentuk yang diperoleh melalui PERKESO; b) Keperluan pelesenan mengehadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperoleh oleh PERKESO; c) Pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan perlesenan; dan d) Pengguna tidak dibenarkan menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	Pengguna Luar

8.33 Perlindungan Rekod

Objektif:

Memastikan pematuhan ke atas undang-undang yang berkaitan dengan rekod.

DP8.33.1 Perlindungan Rekod

Bahagian ICT / Bahagian yang berkaitan hendaklah melindungi rekod daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan kontrak dan/atau perjanjian. Penyimpanan dan pelupusan dokumen sama ada fizikal atau *softcopy* hendaklah dilakukan mengikut kelas dokumen yang berkaitan berdasarkan peraturan dan arahan yang berkuat kuasa dari semasa ke semasa. Rekod-rekod yang penting (dalam bentuk fizikal atau media elektronik) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak dan/atau perjanjian , dan keperluan perniagaan. Perkara yang perlu ditimbangkan ialah: a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; b) Jadual penyimpanan rekod perlu dikenal pasti; dan c) Inventori rekod.	Pengguna Luar

8.34 Privasi dan Perlindungan Maklumat Peribadi

Objektif:

Memastikan pematuhan ke atas undang-undang yang berkaitan dengan aspek keselamatan maklumat peribadi.

DP8.34.1 Perlindungan dan Privasi Data Peribadi	
Hanya terpakai untuk anggota PERKESO sahaja	
DP8.34.2 Perlindungan Data Peribadi	
Penerimaan, pemprosesan, penyimpanan dan perkongsian data peribadi yang diterima hendaklah mematuhi Akta Perlindungan Data Peribadi 2010 (Akta 709) termasuk data yang diterima dalam setiap sistem, laman web atau aplikasi PERKESO.	Pengguna Luar
8.35 Kajian Oleh Pihak Bebas / Pihak Ketiga Berkaitan Keselamatan Maklumat	
Objektif: Memastikan pendekatan yang digunakan oleh PERKESO bersesuaian, cukup dan berkesan secara lebih efektif.	
DP8.35.1 Kajian Semula Keselamatan Maklumat Secara Berkecuali	
Penilaian keselamatan maklumat oleh pengguna luar hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengguna Luar
8.36 Pematuhan Polisi, Peraturan dan Piawaian Untuk Keselamatan Maklumat	
Objektif: Memastikan keselamatan maklumat dilaksanakan mengikut polisi keselamatan siber serta piawaian dan peraturan semasa.	

DP8.36.1 Pematuhan Polisi dan Standard/Piawaian

Hanya terpakai untuk anggota PERKESO sahaja

DP8.36.2 Kajian Semula Pematuhan Teknikal

Hanya terpakai untuk anggota PERKESO sahaja

DP8.36.3 Polisi, Peraturan, Akta Kawalan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

DP8.36.4 Penilaian Tahap Keselamatan

Sistem maklumat hendaklah diuji selaras dengan pematuhan peraturan semasa yang berkuat kuasa. Penilaian ini perlu dilaksanakan sekurang-kurangnya sekali dalam setahun atau mengikut keperluan.	Pengguna Luar

8.37 Prosedur Operasi Yang Perlu Didokumenkan

Objektif:

Prosedur operasi bagi kemudahan pemprosesan maklumat perlu disediakan dan dapat diakses dengan selamat.

DP8.37.1 Penyediaan Prosedur Operasi

Hanya terpakai untuk anggota PERKESO sahaja

9.0 KAWALAN SUMBER MANUSIA

9.1 Tapisan Keselamatan

Objektif:

Memastikan kakitangan dan pihak ketiga memahami tanggungjawab serta peranan dalam aspek keselamatan ICT sepanjang tempoh perkhidmatan mereka.

DP9.1.1 Tapisan Sebelum Pengesahan Pelantikan

Tapisan keselamatan sama ada sebelum atau selepas pengesahan pelantikan hendaklah dijalankan terhadap anggota PERKESO. Tapisan keselamatan turut perlu dilaksanakan kepada pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Pemeriksaan kesahihan maklumat yang merangkumi rujukan individu, *resume*, kelayakan akademik, sijil profesional, identiti pengenalan diri dan rekod jenayah; b) Individu yang dilantik hendaklah kompeten dan bersesuaian untuk peranan yang berkaitan keselamatan maklumat; c) PERKESO hendaklah menjalankan tapisan keselamatan untuk pengguna luar yang terlibat. Ia berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; d) Mengehadkan capaian dan penggunaan aset kerajaan; dan	Pengguna Luar

e) Sekiranya kakitangan atau pengguna luar tidak melepasi tapisan dalam tempoh yang ditetapkan, PERKESO hendaklah mengambil tindakan seperti menangguhkan pelantikan atau membatalkan/menamatkan pelantikan.	

9.2 Terma dan Syarat Perkhidmatan

Objektif:

Memastikan kakitangan dan pihak ketiga memahami tanggungjawab serta peranan dalam keselamatan ICT.

DP9.2.1 Terma dan Syarat Perkhidmatan

Persetujuan mengikat perjanjian dengan pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab PERKESO terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a) Memahami dan bersetuju ke atas tanggungjawab serta hak berkaitan perlindungan keselamatan maklumat; b) Tanggungjawab untuk mengklasifikasikan maklumat dan aset lain yang berkaitan; c) Bertanggungjawab untuk mengendali maklumat daripada pihak berkepentingan; d) Tindakan yang perlu diambil jika tidak mematuhi keselamatan maklumat; e) Memahami peranan dan tanggungjawab dalam keselamatan penyampaian maklumat bagi mengurangkan risiko penyalahgunaan Aset ICT; dan f) Menyatakan dengan lengkap dan jelas peranan serta tanggung jawab pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat dalam menjamin keselamatan aset ICT.	Pengguna Luar

DP9.2.2 Dalam Tempoh Perkhidmatan	
Memastikan pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna luar hendaklah mematuhi semua terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	Pengguna Luar
9.3 Program Kesedaran, Pendidikan dan Latihan Berkaitan Keselamatan Maklumat	
Objektif: Memastikan kakitangan dan pihak ketiga mengambil maklum dan jelas berkaitan tanggungjawab ke atas keselamatan maklumat.	
DP9.3.1 Program Kesedaran Keselamatan Maklumat	
Pengguna Luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai kawalan keselamatan maklumat secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a) Mendapatkan sokongan pengurusan atasan berkaitan keselamatan maklumat; b) Memberi kesedaran berkaitan undang-undang, peraturan, dan perjanjian; c) Memastikan kesedaran, pendidikan dan latihan yang berkaitan dengan Polisi Keselamatan Siber PERKESO, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/ fungsi/	Pengguna Luar

aplikasi/ sistem keselamatan dilaksanakan secara berterusan untuk menyokong pelaksanaan tugas-tugas dan tanggungjawab mereka; d) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat; e) Melaksanakan program kesedaran berkaitan dengan keselamatan maklumat kepada anggota PERKESO dan pengguna luar secara berterusan sepanjang tempoh mereka melaksanakan tugas-tugas dan tanggungjawab mereka; f) Menyediakan program kesedaran keselamatan maklumat setiap tahun; dan g) Memaklumkan senarai perhubungan sekiranya pelanggaran maklumat di kesan oleh pembekal.	

DP9.3.2 Program Latihan dan Pendidikan berkaitan Keselamatan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

9.4 Tindakan Tatatertib

Objektif:

Memastikan kakitangan memahami kesan pelanggaran ke atas keselamatan maklumat mengikut undang-undang atau peraturan lain-lain yang sedang berkuat kuasa.

DP9.4.1 Tindakan Pelanggaran Undang-Undang dan Peraturan

Hanya terpakai untuk anggota PERKESO sahaja

DP9.4.2 Kesalahan Tatatertib

Hanya terpakai untuk anggota PERKESO sahaja

9.5 Tanggungjawab selepas Penamatan atau Pertukaran Pekerjaan

Objektif:

Melindungi kepentingan jabatan semasa proses pertukaran atau penamatan anggota PERKESO.

DP9.5.1 Penamatan atau Pertukaran Tanggungjawab Perkhidmatan

Hanya terpakai untuk anggota PERKESO sahaja

9.6 Perjanjian Kerahsiaan atau Keterdedahan

Objektif:

Memastikan kerahsiaan maklumat yang boleh diakses oleh kakitangan atau pihak ketiga dikenal pasti, didokumenkan, disemak secara berkala dan ditandatangani.

DP9.6.1 Perjanjian Kerahsiaan dan Keterdedahan

Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti, didokumentasi, disemak secara berkala dan ditandatangani oleh wakil PERKESO dan pihak berkepentingan terlibat yang lain. Pihak berkepentingan hendaklah bersetuju dan mematuhi semua keperluan kawalan keselamatan maklumat yang berkuatkuasa dan relevan. Perjanjian kerahsiaan perlu melindungi maklumat berdasarkan undang-undang yang berkuat kuasa terhadap pihak yang berkepentingan dan anggota PERKESO. Kandungan *Non-Disclosure Agreement* yang perlu dipatuhi adalah seperti berikut: a) Definisi maklumat yang perlu dilindungi;	Pengguna Luar

b) Tempoh perjanjian kerahsiaan; c) Tindakan selepas penamatan perjanjian; d) Pengesahan ke atas peminjaman atau akses maklumat perlu dilaksanakan bagi mencegah kebocoran maklumat; e) Pemilikan maklumat, kerahsiaan dan harta intelek yang berkaitan dengan perlindungan kerahsiaan maklumat; f) Kebenaran untuk menggunakan maklumat rahsia rasmi; g) Hak untuk mengaudit dan memantau aktiviti yang melibatkan maklumat rahsia rasmi; h) Proses pemakluman dan pelaporan kebocoran atau pendedahan maklumat; i) Syarat pemulangan atau penghapusan maklumat selepas perjanjian tamat; dan j) Tindakan undang-undang sekiranya perjanjian tidak dipatuhi.	

9.7 Bekerja Jarak Jauh

Objektif:

Memastikan kawalan keselamatan terhadap individu yang bekerja jarak jauh untuk melindungi keselamatan maklumat.

DP9.7.1 Kerja Jarak Jauh

Langkah-langkah kawalan keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di luar premis PERKESO apabila warga agensi/pihak berkepentingan yang bekerja secara jarak jauh (*remote working*). Anggota PERKESO yang bekerja jarak jauh hendaklah : a) Memastikan kawalan keselamatan maklumat PERKESO dipatuhi dan tidak disebarkan kepada pengguna luar; b) Keselamatan fizikal bagi lokasi bekerja jarak jauh seperti di rumah atau lokasi yang dibenarkan sahaja;	Pengguna Luar

c) Kawalan Keselamatan yang merangkumi seperti kabinet fail berkunci, peraturan berkaitan *remote access, clear desk*, pencetakan dan pelupusan maklumat atau aset lain yang berkaitan dan insiden Keselamatan; d) Mengenal pasti lokasi persekitaran fizikal untuk bekerja jarak jauh; e) Menggunakan kawalan komunikasi yang selamatntuk akses ke atas maklumat rahsia rasmi, sistem dan aplikasi kritikal; f) Memastikan kawalan ke atas ancaman daripada pihak lain tanpa kebenaran; g) Mengehadkan konfigurasi rangkaian tanpa wayar (Wi-Fi) dengan membuat pemilihan kategori rangkaian rumah atau rangkaian awam; h) Penggunaan kawalan peralatan atau perisian keselamatan seperti *firewall* dan antivirus; i) Menggunakan kaedah yang selamat untuk pelaksanaan dan memulakan operasi sistem; dan j) Pengesahan dan pengaktifan hak akses yang selamat semasa menggunakan rangkaian luar.	

DP6.7.2 Garis Panduan Kerja Jarak Jauh

Garis panduan kerja jarak jauh hendaklah mematuhi perkara berikut: a) Penggunaan peralatan dan fasiliti penyimpanan maklumat milik persendirian yang bukan di bawah kawalan PERKESO tidak dibenarkan; b) Menetapkan klasifikasi maklumat dan perkhidmatan sistem yang boleh di akses oleh individu bekerja jarak jauh; c) Menyediakan latihan untuk pekerja jarak jauh termasuk yang memberikan khidmat sokongan;	Pengguna Luar

d) Memastikan penggunaan peralatan komunikasi yang sesuai merangkumi kaedah akses jarak jauh yang selamat dan fungsi *device screen locks*; e) Memastikan keselamatan fizikal; f) Menyediakan peraturan serta panduan akses peralatan dan maklumat oleh pihak lain; g) Penyediaan penyelenggaraan sokongan perkakasan, perisian dan insurans; h) Melaksanakan prosedur sandaran dan kesinambungan perkhidmatan; i) Melaksanakan audit dan pemantauan keselamatan; dan j) Membatalkan hak akses dan pemulangan peralatan apabila aktiviti kerja jarak jauh ditamatkan.	

9.8 Pelaporan Insiden Keselamatan Maklumat

Objektif:

Memastikan insiden dikendalikan dengan berkesan bagi meminimumkan impak supaya tidak menjejaskan sistem penyampaian perkhidmatan.

DP9.8.1 Pelaporan Insiden Keselamatan Maklumat

Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT PERKESO. CSIRT PERKESO kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut : a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;	Pengguna Luar

c) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; e) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; f) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka; g) Kesilapan manusia; h) Pelanggaran langkah keselamatan fizikal; i) Perubahan sistem yang belum melalui proses pengurusan perubahan; j) Disyaki jangkitan *malware*; k) Kawalan keselamatan maklumat yang tidak berkesan; l) Pelanggaran sebarang kerahsiaan, integriti atau ketersediaan maklumat; m) Ketidakpatuhan terhadap polisi keselamatan siber; n) Perisian atau perkakasan yang rosak atau tidak berfungsi; o) Penyalahgunaan hak akses; p) Kerentanan; dan q) Percubaan serangan perisian hasad.	
DP9.8.2 Pelaporan Kelemahan Keselamatan Maklumat	
Pengguna Luar terlibat yang lain yang menggunakan sistem dan maklumat agensi dikehendaki mengambil maklum dan melaporkan sebarang insiden atau kelemahan keselamatan maklumat melalui saluran pelaporan yang betul dengan kadar segera.	Pengguna Luar

10.0 KAWALAN FIZIKAL

10.1 Perimeter Keselamatan Fizikal

Objektif:
Memastikan kawalan keselamatan fizikal berkaitan maklumat, premis dan kemudahan ICT.

DP10.1.1 Keselamatan Fizikal

Hanya terpakai untuk anggota PERKESO sahaja

10.2 Kemasukan Fizikal

Objektif:
Melaksanakan kawalan akses masuk kepada maklumat, premis dan kemudahan ICT.

DP10.2.1 Kawalan Kemasukan Fizikal

Kawalan kemasukan fizikal bertujuan memastikan pengurusan keluar masuk ke bangunan PERKESO dilaksanakan secara teratur, selamat dan terkawal. Keperluan berikut hendaklah dipatuhi: a) Menghadkan akses kemasukan ke kawasan berkaitan kepada anggota yang dibenarkan sahaja berdasarkan kelulusan yang ditetapkan; b) Semua pengguna luar hendaklah mempamerkan Pas Keselamatan Pekerja sepanjang waktu bertugas. Pas keselamatan hendaklah dikembalikan kepada PERKESO apabila berlaku pertukaran penempatan, penamatan perkhidmatan atau persaraan;	Pengguna Luar

c) Pengguna Luar/Pelawat wajib mendaftar dan mendapatkan Pas Keselamatan Pelawat di Kaunter Lobi serta mempamerkannya sepanjang berada di bangunan pejabat PERKESO. Pas Keselamatan hendaklah dipulangkan selepas lawatan tamat;

d) Akses penggunaan aset ICT PERKESO hanya dibenarkan kepada pengguna yang menerima kebenaran rasmi;

e) Kehilangan Pas Keselamatan hendaklah dilaporkan serta-merta kepada pihak berkuasa untuk tindakan lanjut;

f) Mengemas kini dan memperkukuh kawalan keselamatan fizikal, terutamanya bagi insiden yang kerap berlaku atau menunjukkan peningkatan risiko;

g) Memastikan semua pintu masuk, termasuk pintu kecemasan, dikawal daripada akses tanpa kebenaran;

h) Pegawai dan kakitangan yang bertugas di luar waktu pejabat hendaklah mendapatkan kebenaran kemasukan terlebih dahulu dan melaporkan kehadiran di Kaunter Lobi sebagai rekod rasmi;

i) Semua pelawat hendaklah merekodkan kehadiran dalam buku daftar pelawat atau sistem pendaftaran pelawat di Kaunter Lobi;

j) Memastikan semua pintu utama dan kawasan terperingkat dilengkapi sistem kawalan akses seperti kad akses, kod pin atau biometrik;

k) Melaksankan pemantauan berterusan melalui Kamera Keselamatan Litar Tertutup (CCTV) di kawasan strategik seperti pintu masuk, lobi, laluan utama dan kawasan terperingkat;

l) Menetapkan larangan membawa masuk peralatan atau bahan tertentu (kamera, perakam suara, peranti storan mudah alih) ke kawasan terperingkat tanpa kelulusan;

m) Menetapkan latihan dan taklimat pematuhan keselamatan kepada semua anggota secara berkala

bagi memastikan kesedaran dan kepatuhan sentiasa berada pada tahap optimum; n) Melaksanakan rondaan keselamatan berkala oleh anggota keselamatan untuk memastikan integriti kawalan akses sentiasa terjamin; dan o) Menyediakan dan mempamerkan papan tanda keselamatan di setiap pintu masuk untuk mengingatkan pengguna mengenai tatacara dan larangan keselamatan.	

DP10.2.2 Kawalan Keselamatan Pelawat

Hanya terpakai untuk anggota PERKESO sahaja

DP10.2.3 Kawasan Penyerahan dan Pemunggahan

Hanya terpakai untuk anggota PERKESO sahaja

10.3 Keselamatan Pejabat, Bilik dan Kemudahan

Objektif:

Memastikan keselamatan dan perlindungan daripada sebarang bentuk pencerobohan, ancaman, kerosakan, kecuaian serta akses yang tidak dibenarkan.

DP10.3.1 Keselamatan Pejabat, Bilik dan Kemudahan ICT

Hanya terpakai untuk anggota PERKESO sahaja

10.4 Pemantauan Keselamatan Fizikal

Objektif:

Memastikan keselamatan fizikal dipantau secara berkesan melalui penggunaan sistem pengawasan dan kawalan bagi mengurangkan risiko pencerobohan, kerosakan, kecurian dan ancaman keselamatan lain.

DP10.4.1 Pemantauan Premis Fizikal

Hanya terpakai untuk anggota PERKESO sahaja

10.5 Perlindungan Terhadap Ancaman Fizikal Dan Bencana

Objektif:

Memastikan infrastruktur yang direka bentuk dilindungi daripada ancaman fizikal dan bencana alam.

DP10.5.1 Perlindungan Terhadap Ancaman Fizikal dan Bencana Alam

Hanya terpakai untuk anggota PERKESO sahaja

10.6 Bekerja di Kawasan Selamat

Objektif:

Memastikan maklumat dan Aset ICT berada di kawasan yang selamat daripada gangguan atau kerosakan daripada pekerja sekitarnya.

DP10.6.1 Bekerja di Kawasan Selamat

Hanya terpakai untuk anggota PERKESO sahaja

10.7 Meja Kosong dan Skrin Kosong

Objektif:

Memastikan kawalan capaian maklumat yang tidak dibenarkan di atas meja atau di paparan skrin atau di mana-mana lokasi yang boleh diakses semasa dan di luar waktu pejabat.

DP10.7.1 Dasar Meja Kosong dan Skrin Kosong

Hanya terpakai untuk anggota PERKESO sahaja

DP10.7.2 Peralatan Pengguna Tanpa Kawalan

Hanya terpakai untuk anggota PERKESO sahaja

10.8 Penempatan dan Perlindungan Peralatan ICT

Objektif:

Memastikan peralatan ICT ditempatkan di kawasan yang selamat dan dilindungi daripada sebarang bentuk pencerobohan dan ancaman.

DP10.8.1 Penempatan dan Perlindungan Peralatan ICT

Hanya terpakai untuk anggota PERKESO sahaja

10.9 Keselamatan Aset di Luar Premis

Objektif:

Memastikan Keselamatan Aset ICT yang dibawa keluar dari premis dilindungi.

DP10.9.1 Peralatan ICT di Luar Premis

Hanya terpakai untuk anggota PERKESO sahaja

10.10 Media Storan

Objektif:

Memastikan media storan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

DP10.10.1 Pengurusan Media Storan Mudah Alih

Hanya terpakai untuk anggota PERKESO sahaja

DP10.10.2 Pelupusan Media

Hanya terpakai untuk anggota PERKESO sahaja

DP10.10.3 Pengalihan Aset

Hanya terpakai untuk anggota PERKESO sahaja

10.11 Perkhidmatan Sokongan

Objektif:
Memastikan kawalan ke atas fasiliti sokongan dilindungi daripada gangguan.

DP10.11.1 Fasiliti Sokongan

Hanya terpakai untuk anggota PERKESO sahaja

10.12 Keselamatan Pengkabelan

Objektif:
Memastikan kabel rangkaian dan kuasa elektrik dilindungi daripada gangguan dan pencerobohan.

DP10.12.1 Keselamatan Kabel

Kabel kuasa elektrik dan rangkaian yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Perkara yang hendaklah dipatuhi adalah seperti yang berikut: a) Kabel termasuk kabel elektrik dan rangkaian yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. b) Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut: i. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; ii. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;	Pengguna Luar

iii. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan iv. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

10.13 Penyelenggaraan Peralatan

Objektif:

Memastikan semua peralatan berkaitan perkhidmatan ICT diselenggarakan untuk mengelakkan gangguan operasi.

DP10.13.1 Penyelenggaraan Peralatan

Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau selepas tamat tempoh jaminan; b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan;	Pengguna Luar

f) Menyimpan rekod penyelenggaraan pencegahan dan pemulihan; g) Menyelia kerja-kerja penyelenggaraan yang dilakukan oleh pengguna luar; h) Mengawal akses bagi penyelenggaraan yang dilaksanakan secara jarak jauh (*remote*); i) Melaksanakan kawalan keselamatan ke atas penyelenggaraan peralatan di luar premis; dan j) Melaksanakan kaedah yang bersesuaian untuk pelupusan atau penggunaan semua peralatan.	

10.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Objektif:

Memastikan kaedah pelupusan dan penggunaan semula peralatan dilaksanakan mengikut peraturan yang berkuat kuasa.

DP10.14.1 Pelupusan yang Selamat atau Penggunaan Semula Peralatan

Hanya terpakai untuk anggota PERKESO sahaja

DP10.14.2 Penggunaan Semula Peralatan

Hanya terpakai untuk anggota PERKESO sahaja

11.0 KAWALAN TEKNOLOGI

11.1 Aset ICT Pengguna

Objektif:
Melindungi maklumat yang terdapat dalam Aset ICT pengguna.

DP11.1.1 Polisi Peranti *Endpoint*

Hanya terpakai untuk anggota PERKESO sahaja

DP11.1.2 Penggunaan Aset ICT

Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan jenis dan klasifikasi maklumat yang boleh diakses, diproses atau disimpan dalam Aset ICT pengguna; b) Memastikan semua Aset ICT pengguna didaftarkan; c) Memastikan pengguna bertanggungjawab ke atas Aset ICT; d) Memastikan perisian yang boleh dipasang pada Aset ICT pengguna telah mendapat kelulusan; e) Memastikan Aset ICT pengguna di konfigurasi dengan versi perisian atau patches terkini; f) Menetapkan peraturan bagi sambungan ke rangkaian awam, atau rangkaian lain di luar premis menggunakan Aset ICT pengguna; g) Mematuhi kawalan capaian menggunakan Aset ICT pengguna; h) Memastikan Aset ICT pengguna melaksanakan enkripsi bagi penyimpanan maklumat PERKESO; i) Memastikan Aset ICT pengguna mempunyai perisian antivirus;	Pengguna Luar

j) Memastikan peraturan berkaitan *remote disabling*, *deletion* atau *lockout* di patuhi; k) Memastikan pelaksanaan sandaran bagi maklumat PERKESO yang disimpan di dalam Aset ICT pengguna; l) Menggunakan perkhidmatan web dan aplikasi yang dibenarkan sahaja; m) Melaksanakan analisa penggunaan Aset ICT pengguna; n) Menyahaktifkan USB port sekiranya perlu; o) Memastikan pengasingan (*hard disk partition*) data dan perisian pada Aset ICT pengguna; dan p) PERKESO berhak untuk mengambil tindakan pentadbiran yang sewajarnya seperti penamatan akses sekiranya didapati anggota tidak mematuhi peraturan dalam polisi ini.	

DP11.1.3 Peralatan Pengguna Tanpa Kawalan

Hanya terpakai untuk anggota PERKESO sahaja

DP11.1.4 Mengaktifkan Kawalan Keselamatan

Hanya terpakai untuk anggota PERKESO sahaja

11.2 Kebenaran Hak Akses

Objektif:
Memastikan akses pengguna, komponen perisian dan perkhidmatan yang disediakan hanya diberikan kepada pengguna yang dibenarkan.

DP11.2.1 Hak Akses Istimewa

Hanya terpakai untuk anggota PERKESO sahaja

11.3 Kawalan Akses Maklumat

Objektif:

Memastikan hanya akses yang dibenarkan ke atas maklumat dan aset yang berkaitan.

DP11.3.1 Akses Maklumat dan Aset Berkaitan

Hanya terpakai untuk anggota PERKESO sahaja

DP11.3.2 Akses Maklumat Rahsia Rasmi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.3.3 Kawalan Pengurusan Akses Maklumat dan Aset yang Berkaitan

Hanya terpakai untuk anggota PERKESO sahaja

11.4 Akses Kepada Kod Sumber

Objektif:

Akses baca dan tulis kepada kod sumber, perisian pembangunan dan perpustakaan perisian (software libraries) hendaklah diuruskan dengan sewajarnya.

DP11.4.1 Kawalan Kod Sumber

Hanya terpakai untuk anggota PERKESO sahaja

11.5 Pengesahan Selamat

Objektif:

Memastikan pengguna atau individu menggunakan pengesahan yang sah untuk akses kepada sistem aplikasi dan perkhidmatan yang disediakan.

DP11.5.1 Pengesahan Prosedur Log Masuk Yang Selamat

Hanya terpakai untuk anggota PERKESO sahaja

11.6 Pengurusan Kapasiti

Objektif:

Memastikan pengurusan kapasiti ke atas kemudahan pemprosesan maklumat, sumber manusia, keperluan pejabat dan lain-lain dikenal pasti.

DP11.6.1 Pengurusan Kapasiti

Hanya terpakai untuk anggota PERKESO sahaja

DP11.6.2 Peningkatan Kapasiti

Hanya terpakai untuk anggota PERKESO sahaja

DP11.6.2 Pengurangan Kapasiti

Hanya terpakai untuk anggota PERKESO sahaja

8.7 Perlindungan Terhadap Perisian Hasad

Objektif:

Memastikan perisian dan aset berkaitan ICT dilindungi daripada perisian hasad (*malware*). Perlindungan terhadap perisian hasad hendaklah berdasarkan maklumat pengesanan dan pembaikan perisian hasad tersebut, kesedaran keselamatan, akses sistem yang sesuai serta kawalan pengurusan perubahan.

DP11.7.1 Perlindungan daripada Perisian Hasad

Hanya terpakai untuk anggota PERKESO sahaja

11.8 Pengurusan Teknikal Ke Atas Kerentanan

Objektif:

Mencegah eksploitasi kerentanan teknikal dalam sistem maklumat. Maklumat mengenai kelemahan teknikal perlu dikenal pasti, kelemahan organisasi perlu dinilai dan langkah-langkah yang sesuai perlu diambil.

DP11.8.1 Mengenal Pasti Kerentanan Teknikal

Hanya terpakai untuk anggota PERKESO sahaja

DP11.8.2 Penilaian Kerentanan Teknikal

Hanya terpakai untuk anggota PERKESO sahaja

DP11.8.3 Panduan Menangani Kelemahan Teknikal

Hanya terpakai untuk anggota PERKESO sahaja

11.9 Pengurusan Konfigurasi

Objektif:

Memastikan konfigurasi perkakasan, perisian, perkhidmatan, dan rangkaian ICT berfungsi dengan baik dan mengambil kira aspek keselamatan.

DP11.9.1 Pengurusan Konfigurasi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.9.2 Pemantauan Konfigurasi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.9.3 Amalan Baik Pengurusan Konfigurasi

Hanya terpakai untuk anggota PERKESO sahaja

11.10 Penghapusan Maklumat

Objektif:

Memastikan penghapusan maklumat dilaksanakan mematuhi keperluan undang-undang dan peraturan yang berkuat kuasa.

DP11.10.1 Penghapusan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

11.11 Penyamaran Data

Objektif:

Memastikan paparan data sensitif dihadkan mengikut peraturan, keperluan organisasi dan perundangan yang berkuat kuasa.

DP11.11.1 Teknik Penyamaran Data

Hanya terpakai untuk anggota PERKESO sahaja

DP11.11.2 Pelaksanaan Penyamaran Data

Hanya terpakai untuk anggota PERKESO sahaja

11.12 Pencegahan Ketirisan Data

Objektif:

Memastikan ketirisan data dikenal pasti dan dihalang daripada berlaku. Langkah pencegahan ketirisan data hendaklah digunakan pada sistem, rangkaian dan perkakasan ICT lain yang memproses, menyimpan atau menghantar maklumat.

DP11.12.1 Pencegahan Ketirisan Data

Hanya terpakai untuk anggota PERKESO sahaja

11.13 Sandaran Maklumat

Objektif:

Memastikan salinan sandaran maklumat, perisian dan sistem di selenggara serta diuji secara berkala.

DP11.13.1 Sandaran Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

11.14 Lewahan bagi Kemudahan Pemprosesan Maklumat

Objektif:

Memastikan ketersediaan kemudahan operasi ICT.

DP11.14.1 Lewahan bagi Kemudahan Pemprosesan Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

11.15 Merekodkan Log

Objektif:

Memastikan maklumat log di rekodkan dan dianalisis bagi menghalang daripada akses yang tidak dibenarkan.

DP11.15.1 Polisi Log Aktiviti

Hanya terpakai untuk anggota PERKESO sahaja

DP11.15.2 Kawalan Perlindungan Log

Hanya terpakai untuk anggota PERKESO sahaja

DP11.15.3 Analisis Log

Hanya terpakai untuk anggota PERKESO sahaja

DP11.15.4 Log Pentadbir dan Pengendali

Hanya terpakai untuk anggota PERKESO sahaja

11.16 Aktiviti Pemantauan

Objektif:
Memastikan insiden keselamatan maklumat dapat dikesan dan pemantauan dilaksanakan secara berkala.

DP11.16.1 Aktiviti Pemantauan

Hanya terpakai untuk anggota PERKESO sahaja

DP11.16.2 Pemantauan Aktiviti Anomali

Hanya terpakai untuk anggota PERKESO sahaja

DP11.16.3 Kawalan Pemantauan Aktiviti Anomali

Hanya terpakai untuk anggota PERKESO sahaja

11.17 Penyeragaman Waktu

Objektif:
Memastikan analisis berkaitan aktiviti keselamatan serta data lain yang direkodkan selari dengan Waktu Piawai Malaysia (MST).

DP11.17.1 Penyeragaman Waktu

Hanya terpakai untuk anggota PERKESO sahaja

11.18 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa

Objektif:

Memastikan penggunaan program utiliti tidak menjejaskan kawalan keselamatan maklumat bagi sistem aplikasi.

DP11.18.1 Penggunaan Program Utiliti

Hanya terpakai untuk anggota PERKESO sahaja

11.19 Pemasangan Perisian pada Sistem yang Beroperasi

Objektif:

Memastikan penggunaan perisian yang dibenarkan pada peralatan ICT.

DP11.19.1 Pemasangan Perisian pada Sistem yang Beroperasi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.19.2 Sekatan ke atas Pemasangan Perisian

Hanya terpakai untuk anggota PERKESO sahaja

11.20 Keselamatan Rangkaian

Objektif:

Memastikan pengurusan keselamatan perkhidmatan rangkaian dilaksanakan bagi melindungi maklumat dan kemudahan ICT daripada ancaman.

DP11.20.1 Kawalan Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

DP11.20.2 Keselamatan Peranti Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

11.21 Keselamatan Perkhidmatan Rangkaian

Objektif:

Memastikan keperluan, mekanisme keselamatan, dan tahap perkhidmatan rangkaian dilaksanakan serta dipantau.

DP11.21.1 Panduan Perkhidmatan Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

DP11.21.2 Keselamatan Perkhidmatan Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

DP11.21.3 Peralatan dalam Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

DP11.21.4 Capaian ke *PORT* Untuk Tujuan Diagnostik

Hanya terpakai untuk anggota PERKESO sahaja

11.22 Pengasingan Rangkaian

Objektif:

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

DP11.22.1 Panduan Pengasingan Rangkaian

Hanya terpakai untuk anggota PERKESO sahaja

11.23 Penyaringan Web

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

DP11.23.1 Kawalan Penyaringan Web

Hanya terpakai untuk anggota PERKESO sahaja

11.24 Penggunaan Kriptografi

Objektif:
Memastikan penggunaan kriptografi untuk melindungi kerahsiaan dan integriti maklumat berdasarkan keperluan PERKESO dengan mematuhi keperluan undang-undang yang berkaitan.

DP11.24.1 Polisi Penggunaan Kawalan Kriptografi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.24.2 Pengurusan Kunci Kriptografi

Hanya terpakai untuk anggota PERKESO sahaja

DP11.24.3 Penggunaan Kriptografi

Hanya terpakai untuk anggota PERKESO sahaja

11.25 Kitar Hayat Pembangunan Yang Selamat

Objektif:

Memastikan pembangunan sistem aplikasi mengguna pakai kitar hayat pembangunan yang selamat.

DP11.25.1 Dasar Pembangunan Sistem Yang Selamat

Hanya terpakai untuk anggota PERKESO sahaja

DP11.25.2 Kitar Hayat Pembangunan Sistem Yang Selamat

Hanya terpakai untuk anggota PERKESO sahaja

11.26 Keperluan Keselamatan Aplikasi

Objektif:

Memastikan semua keperluan keselamatan maklumat dikenal pasti dan ditangani semasa pembangunan atau penambahbaikan sistem aplikasi.

DP11.26.1 Keperluan Keselamatan Sistem Aplikasi

Spesifikasi reka bentuk aplikasi hendaklah mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk *off-the-shelf* diperolehi, pengguna luar perlu dimaklumkan berkenaan keperluan keselamatan produk. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Memastikan pengguna mempunyai tahap akses yang dibenarkan; b) Mengenal pasti jenis maklumat dan tahap klasifikasi yang akan diproses oleh sistem aplikasi; c) Membezakan had akses kepada data dan fungsi dalam sistem aplikasi;	Pengguna Luar

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; h) Memastikan data yang diproses dan dipindahkan dilindungi; i) Memastikan komunikasi antara semua pihak di enkripsi dengan selamat; j) Melaksanakan pengesahan input; k) Mengawal kelulusan yang dijana oleh Sistem Aplikasi seperti mengehadkan kelulusan atau menetapkan lebih daripada 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; dan p) Pengendalian mesej ralat.	

DP11.26.2 Transaksi Perkhidmatan Dalam Talian

Maklumat yang terlibat dalam urusan perkhidmatan dalam talian hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang papar mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:	Pengguna Luar

a) Memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem; b) Memastikan penggunaan mekanisme seperti digital *signature, hashing* dan lain-lain untuk mengesahkan identiti penghantar dan penerima semasa pertukaran data; c) Memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi; d) Memastikan semua pihak memahami aspek kerahsiaan, integriti, serta bukti penghantaran dan penerimaan dokumen; e) Memastikan perkhidmatan sistem aplikasi menggunakan *Secure Socket Layer* (SSL) dalam setiap transaksi; f) Menetapkan tempoh transaksi yang disimpan; dan g) Keperluan insurans dan kontrak perjanjian Pihak yang mengeluarkan tandatangan digital ialah yang diiktiraf oleh Kerajaan.	

DP11.26.3 Aplikasi Pesanan dan Pembayaran Elektronik

Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Mengekalkan kerahsiaan dan integriti maklumat pesanan atau pembayaran; b) Mengesahkan maklumat pembayaran oleh pelanggan; c) Mengelakkan kehilangan atau duplikasi maklumat transaksi; d) Menyimpan maklumat transaksi di lokasi yang selamat dan tidak boleh diakses oleh orang ramai; dan e) Menggunakan tandatangan atau sijil digital yang sah dan dikeluarkan oleh pihak yang diberi kuasa (*authority*).	Pengguna Luar

11.27 Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat

Objektif:

Prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumenkan, dikaji dan diguna pakai ke atas semua pembangunan sistem aplikasi.

DP8.27.1 Prinsip Kejuruteraan Sistem yang Selamat

Prinsip untuk kejuruteraan sistem yang selamat hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk aktiviti pembangunan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a) Menyediakan kawalan keselamatan yang diperlukan untuk melindungi maklumat dan sistem aplikasi daripada ancaman yang dikenal pasti; b) Mempunyai keupayaan kawalan keselamatan untuk mencegah, mengesan atau melaksanakan tindakan ke atas insiden keselamatan; c) Memastikan semua maklumat rahsia rasmi di enkripsi (*encryption*); d) Mengenal pasti keperluan kawalan keselamatan yang akan dilaksanakan; e) Melaksanakan kawalan keselamatan terhadap individu yang berkaitan; f) Memastikan prinsip kejuruteraan mengaplikasikan reka bentuk keselamatan (*security architecture*); g) Memastikan kawalan keselamatan infrastruktur seperti penggunaan *public key infrastructure* (PKI), *identity and*	Pengguna Luar

access management (IAM), pencegahan kebocoran data dan pengurusan akses dinamik; h) Mempunyai kepakaran untuk membangunkan dan menyelenggarakan sistem aplikasi selari dengan teknologi yang digunakan atau dipilih; i) Mengambil kira keperluan kos, masa dan cabaran dalam memenuhi keperluan keselamatan; j) Mengguna pakai konsep amalan terbaik (*best practise*); dan k) Melaksanakan *Security Posture Assessment* (SPA) dan *hardening* ke atas sistem aplikasi sebelum ia digunakan atau diletakkan dalam persekitaran produksi.	

DP11.27.2 Prinsip "*Zero Trust*"

Perkara yang perlu diambil kira adalah seperti berikut: a) Kawalan keselamatan tidak boleh bergantung sepenuhnya kepada peralatan keselamatan rangkaian; b) Menyemak dan mengesahkan identiti bagi semua akses ke sistem aplikasi; c) Memastikan sistem aplikasi menggunakan fungsi enkripsi; d) Menyemak dan mengesahkan semua permohonan akses yang diterima; e) Memberikan kategori akses paling minimum kepada pengguna; dan f) Menggunakan pengesahan keselamatan ketika log masuk atau transaksi yang melibatkan sistem aplikasi seperti *multi factor authentication* (MFA), *captcha, security phrase* dan *secure transaction authorisation code* (TAC).	Pengguna Luar

11.28 Pengekodan Selamat

Objektif:

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

DP11.28.1 Kawalan Capaian Kepada Kod Sumber

Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik PERKESO kecuali aplikasi yang diperoleh secara *off-the-shelf* atau secara langganan. **Perancangan Sebelum Pengekodan** Prinsip pengekodan selamat hendaklah digunakan untuk pembangunan baru dan dalam senario penggunaan semula. Prinsip-prinsip ini hendaklah diterapkan dalam aktiviti pembangunan baik dalam PERKESO dan untuk produk serta perkhidmatan yang dibekalkan oleh PERKESO kepada pihak lain. Perancangan dan prasyarat sebelum pengekodan hendaklah merangkumi perkara seperti berikut tetapi tidak terhad kepada: a) Pembangunan sistem aplikasi sama ada secara dalaman (*in-house*) atau luaran (*outsource*) hendaklah menggunakan pengekodan selamat berdasarkan kepada peraturan dan keperluan yang dikuatkuasakan; b) Memastikan amalan dan kelemahan pengekodan yang berlaku sebelum ini dijadikan sebagai sumber rujukan supaya kelemahan keselamatan maklumat yang sama tidak berulang; c) Menggunakan perisian Pembangunan seperti *Integrated Development Environments* (IDE) untuk membantu pengekodan selamat; d) Penggunaan persekitaran pembangunan semasa fasa pembangunan sistem aplikasi;	Pengguna Luar

e) Memastikan penggunaan perisian pembangunan yang terkini;
f) Memastikan pengaturcaraan atau pengguna luar yang dilantik mempunyai kemahiran dalam pembangunan sistem aplikasi menggunakan pengekodan selamat; dan
g) Memastikan arkitektur, reka bentuk dan standard pengekodan digunakan dalam persekitaran yang selamat.

Perancangan Semasa Pengekodan

Pertimbangan semasa pengekodan hendaklah merangkumi:

a) Memastikan penggunaan teknik dan struktur pengekodan selamat bagi bahasa pengaturcaraan yang digunakan seperti *pair programming, refactoring* dan *test-driven development*;
b) Merekodkan dan memperbetulkan kelemahan kod sumber yang boleh terdedah kepada ancaman daripada dieksploitasi;
c) Menggunakan perisian yang terkini dan tidak tamat tempoh *end of support* (EOS);
d) Memastikan tidak menggunakan Teknik Pembangunan yang tidak selamat seperti *hard-coded passwords, unapproved code samples* dan *unauthenticated web services*;
e) Melaksanakan pengujian keselamatan maklumat dan tindakan pembaikan.
f) Memastikan keupayaan integrasi dengan sistem maklumat yang lain;
g) Sebelum sistem aplikasi digunakan, perkara seperti di bawah hendaklah dilaksanakan:
   i. Memastikan hak akses minimum pengguna;
   ii. Melaksanakan analisa berkaitan kesalahan umum kod pengaturcaraan dan merekodkan tindakan pembetulan

Semakan dan penyelenggaraan

Pertimbangan selepas kod telah beroperasi:

a) Memastikan *patches* dan *security updates* perisian sentiasa dikemas kini;
b) Kelemahan keselamatan maklumat yang dilaporkan hendaklah diambil tindakan;
c) Ralat dan cubaan serangan hendaklah direkodkan serta disemak secara berkala bagi penambahbaikan ke atas kod pengaturcaraan sekiranya perlu; dan
d) Kod sumber hendaklah dilindungi daripada akses dan gangguan yang tidak dibenarkan seperti menggunakan fungsi kawalan versi (*version control*).

Sekiranya menggunakan *libraries* luaran, perkara seperti di bawah hendaklah dilaksanakan:

a) Memastikan *libraries* luaran yang digunakan adalah versi terkini; atau
b) Menggunakan komponen seperti pengesahan kriptografi yang telah disahkan dan stabil;
c) Memastikan lesen, keselamatan dan komponen luaran yang sah;
d) Memastikan *libraries* boleh diselenggarakan dan diperoleh daripada sumber yang dipercayai; atau
e) Ketersediaan sumber yang mencukupi untuk rujukan pembangunan jangka panjang.

Sekiranya *software package* perlu ditambah baik, perkara seperti di bawah hendaklah dipastikan:

a) Risiko kepada fungsi kawalan sedia ada dan integriti perisian tersebut;
b) Perlu mendapatkan kebenaran persetujuan daripada pengguna luar;
c) Keperluan untuk mendapatkan perubahan versi terkini;

d) Implikasi yang akan berlaku sekiranya tanggungjawab penyelenggaraan diberikan kepada PERKESO; dan e) Keserasian (*compatibility*) dengan perisian yang lain.	

11.29 Pengujian dan Penerimaan Keselamatan Sistem

Objektif:

Memastikan keperluan keselamatan maklumat dipenuhi semasa sistem aplikasi diguna pakai dalam persekitaran sebenar.

DP11.29.1 Pengujian Keselamatan Sistem

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Fungsi keselamatan sistem aplikasi hendaklah diuji semasa fasa Pembangunan seperti pengesahan pengguna, kawalan akses, penggunaan kriptografi 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 semua sistem aplikasi baharu atau penambahbaikan sistem aplikasi; d) Menyemak dan mengesahkan data sebelum dikunci masuk dalam sistem aplikasi bagi menjamin ketepatan maklumat; dan e) Melaksanakan semakan dan pengesahan ke atas output data yang dihasilkan oleh sistem aplikasi. Maklumat lanjut berkaitan pengujian keselamatan sistem boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 *Software Testing Standard*.	Pengguna Luar

DP11.29.2 Pengujian Penerimaan Sistem	
Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Menyediakan jadual aktiviti pengujian; b) Menyediakan input dan output yang dijangka supaya memenuhi senarai syarat yang telah ditentukan; c) Menetapkan kriteria untuk menilai keputusan; d) Memastikan proses kerja sistem aplikasi memenuhi keperluan pengguna; e) Melaksanakan pengujian fungsi ke atas sistem aplikasi menggunakan data palsu (*dummy input*); f) Melaksanakan keputusan pengujian yang memerlukan tindakan lanjut sekiranya diperlukan; g) Melaksanakan integrasi dan pengujian dengan sistem aplikasi yang lain sekiranya berkaitan; dan h) Melaksanakan ujian prestasi (*performance test*) dan ujian tekanan (*stress test*).	Pengguna Luar

DP11.29.3 Pengujian Bebas Pembangunan Dalaman dan Luaran	
Pengujian perlu dilaksanakan oleh selain daripada pasukan pembangunan sistem aplikasi. Perkara berikut perlu diambil kira seperti: a) Melaksanakan aktiviti semakan kod pengaturcaraan untuk mengenal pasti kelemahan termasuk input dan ralat yang tidak dijangka; b) Melaksanakan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem aplikasi;	Pengguna Luar

c) Melaksanakan pengujian penembusan (*penetration testing*) untuk mengenal pasti reka bentuk dan kod sumber tidak selamat; d) Penilaian sesuatu perolehan hendaklah dilaksanakan sebelum bekalan dan perkhidmatan diterima; e) Perjanjian bersama pengguna luar perlu mengandungi keperluan keselamatan; f) Pembangunan secara luaran (*outsource*) atau pembelian komponen hendaklah mematuhi tatacara perolehan yang sedang berkuatkuasa; dan g) Persekitaran pengujian hendaklah sama dengan persekitaran sebenar supaya pengujian tersebut tidak boleh disangkal dan boleh dipercayai.	

11.30 Pembangunan Secara Luaran

Objektif:

Pembangunan sistem aplikasi yang dilaksanakan oleh pihak ketiga perlu dikawal selia dan dipantau bagi memastikan keselamatan maklumat dipatuhi.

DP11.30.1 Pembangunan Sistem Secara Luaran

PERKESO hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara luaran oleh pengguna luar. Kod sumber *(source code)* adalah menjadi **HAK MILIK** PERKESO kecuali sistem atau aplikasi yang diperolehi secara *off-the-shelf*. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Perjanjian lesen, kod sumber ialah **HAK MILIK PERKESO** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi menggunakan sumber luar; b) Bagi semua perkhidmatan yang disediakan oleh sumber luar, *Software as a Service* (SaaS) yang mengendalikan	Pengguna Luar

Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori. **Pengguna Luar hendaklah membenar hak PERKESO mencapai kod sumber dan melaksanakan pengolahan risiko**;

c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;
d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;
e) Mengguna pakai prinsip dan tatacara *eskrow*;
f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian;
g) Penyediaan model ancaman (*threat modelling*) untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima;
h) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk mengawal kehadiran kandungan berniat jahat semasa penghantaran;
i) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk melindungi daripada kelemahan yang
j) diketahui;
k) Keperluan keselamatan untuk persekitaran pembangunan; dan
l) Mempertimbangkan kesan perundangan yang berlaku.

11.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Pengeluaran

Objektif:

Memastikan keselamatan maklumat dalam semua persekitaran ICT dilindungi daripada ancaman oleh pihak tidak dibenarkan.

DP11.31.1 Pengasingan Persekitaran ICT

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) Mewujudkan prosedur keperluan sumber bagi penyediaan persekitaran untuk pembangunan, pengujian dan sebenar; b) Mengasingkan persekitaran sebenar dengan pembangunan dalam domain yang berbeza seperti *virtual* atau fizikal; c) Menetapkan, merekodkan dan melaksanakan peraturan serta pengesahan untuk penggunaan sistem aplikasi atau perisian daripada persekitaran pembangunan kepada persekitaran sebenar; d) Melaksanakan pengujian ke atas perubahan sistem aplikasi di persekitaran pengujian sebelum digunakan dalam persekitaran sebenar; e) Tidak menggunakan maklumat sebenar pada persekitaran pembangunan atau persekitaran pengujian kecuali dengan kawalan keselamatan; f) Memastikan *compilers*, editor dan *tools* pembangunan atau program utiliti lain tidak boleh diakses daripada persekitaran sebenar apabila tidak diperlukan lagi; g) Merekodkan semua penggunaan sumber yang dilaksanakan; dan h) Memantau pelaksanaan penggunaan sumber bagi tujuan perancangan kapasiti.	Pengguna Luar

DP11.31.2 Langkah Keselamatan bagi Persekitaran Pembangunan dan Pengujian

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan dan pengujian sistem yang selamat dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. PERKESO hendaklah menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a) Mengemas kini *patches*, 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; dan e) Menyediakan sandaran (*backup*) mengikut persekitaran.	Pengguna Luar

11.32 Pengurusan Perubahan

Objektif:

Memastikan pengurusan perubahan dalam persekitaran ICT dilaksanakan dengan mengambil kira kawalan keselamatan maklumat.

DP11.32.1 Pengurusan Perubahan

Perubahan dalam organisasi, proses bisnes, 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	Pengguna Luar

mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini 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; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
DP11.32.2 Prosedur Kawalan Perubahan Sistem	
Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a) Merancang dan menilai impak yang mungkin berlaku ke atas pihak lain yang mempunyai kepentingan atau kebergantungan; b) Memastikan perubahan yang dilaksanakan telah mendapat kelulusan; c) Memastikan perubahan yang dilaksanakan dimaklumkan kepada pihak berkepentingan; d) Perubahan atau pengubahsuaian ke atas perkakasan, perisian atau sistem aplikasi hendaklah diuji, direkodkan dan disahkan sebelum diguna pakai; e) Memastikan pelaksanaan perubahan mengambil kira perancangan pembangunan;	Pengguna Luar

f) Memastikan prosedur pembentukan semula (*fallback*) dilaksanakan sebagai pelan perancangan luar jangka (*contingency*);
g) Merekodkan semua perubahan yang dilaksanakan;
h) Memastikan manual operasi pengguna dan sistem aplikasi diubah mengikut keperluan;
i) Memastikan prosedur pelan kesinambungan perkhidmatan dan pemulihan ICT diubah mengikut keperluan;
j) Semua aspek mengawal pelaksanaan perubahan menggunakan prosedur kawalan perubahan;
k) Setiap perubahan kepada pengoperasian sistem perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap keselamatan maklumat;
l) Perubahan kepada kod pengaturcaraan (*source code*) sistem aplikasi perlu dihadkan kepada pengguna yang dibenarkan; dan
m) Memastikan aktiviti seperti memasang, menyelenggarakan, menghapus dan mengemas kini mana-mana komponen ICT hendaklah mendapatkan kelulusan.

DP11.32.3 Penilaian Teknikal Sistem Aplikasi Selepas Perubahan

Hanya terpakai untuk anggota PERKESO sahaja

DP11.32.4 Kawalan Perubahan Kepada Perisian

Hanya terpakai untuk anggota PERKESO sahaja

11.33 Maklumat Pengujian

Objektif:

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

DP11.33.1 Panduan Penggunaan Data

Hanya terpakai untuk anggota PERKESO sahaja

11.34 Perlindungan Sistem Maklumat Semasa Pengujian Audit

Objektif:

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

DP11.34.1 Kawalan Audit Sistem Maklumat

Hanya terpakai untuk anggota PERKESO sahaja

LAMPIRAN A

FORMAT

PERMOHONAN PANDANGAN / NASIHAT UNDANG-UNDANG

A. LATAR BELAKANG

_____

_____

_____

_____

B. ISU YANG DIMOHON PANDANGAN / NASIHAT UNDANG-UNDANG

_____

_____

_____

_____

C. ARAHAN / PEKELILING / GARIS PANDUAN / PERJANJIAN / DOKUMEN LAIN YANG BERKAITAN

_____

_____

_____

_____

D. SYOR

_____

_____

_____

_____

E. KESIMPULAN

_____

_____

_____

_____

LAMPIRAN B

Non-Disclosure Agreement

This Non-Disclosure Agreement is made between:

PERTUBUHAN KESELAMATAN SOSIAL, Management Services Division, 11th Floor, Menara PERKESO, 281, Jalan Ampang 50538 Kuala Lumpur ("PERKESO"): and

The Party specified below:

_____

_____

_____

_____

"Vendor" ☐ "Agency" ☐

Recital:

A. Pursuant to the agreement/letter of intent _____ entered/date into between _____ and _____ date _____, the parties to the agreement further agree to enter into this agreement for the purpose of data security in relation to the data/information obtained in the course of business relationship between the parties with the first agreement.

B. In the course of the business relationship between PERKESO and Vendor/Agency, Vendor/ Agency will have access to confidential and/or proprietary information of PERKESO.

C. In order to protect such Confidential Information, Vendor/Agency agrees to execute this Agreement.

---

1. Confidential Information as used in this Agreement means information relating to PERKESO including without limitation (i) pricing and costing information and general financial data , technical information and know-how, current and future product information, customer names and data, information relating to product plans, designs, developments, software configuration, processes and developments, forecasts, practices, methodologies, marketing, financial and business plans, documents, drawings, reports, inventions, samples (ii) any information marked "Confidential" or "Proprietary" or the equivalent, including classifications under the Official Secrets Act 1972 (Act 88) as "Rahsia Besar," "Rahsia," "Sulit," "Terhad," or "Terbuka," at the time of disclosure; at the time of disclosure and (iii) any information which can reasonably be regarded as confidential. Confidential Information may include information belonging to a third party such as customers or suppliers, or potential customers or suppliers, of PERKESO, and shall include information protected under the Official Secrets Act 1972 (Act 88).

2. Confidential Information shall include all Confidential Information existing or conveyed or accessible to, used by or in possession of Vendor/ Agency prior to or subsequent to the date of this Agreement. For the avoidance of doubt, Confidential Information shall include all data including employees and employers information, extracts, copies or reproductions in any media, not restricted to photocopies and recordings, or the conversion from any media to other media.

3. Except as otherwise agreed in writing, the obligations under this Agreement shall continue indefinitely.

4. Vendor/Agency shall receive and hold the Confidential Information in strictest confidence, and install and maintain sufficient processes, precautions and mechanisms for the security and confidentiality of the Confidential Information. Confidential Information shall not be disclosed to any person and may only be disclosed to Vendor/Agency's employees who are under non-disclosure obligations no less restrictive than in this Agreement, on a need-to-know basis. Vendor/ Agency will advise its employees who receive Confidential Information of its confidential nature and shall ensure that each of its employee who has access to the Confidential Information shall execute an undertaking in the form as specified by PERKESO. Vendor/Agency shall cooperate with PERKESO in fully enforcing any obligations against its employees.

5. Vendor/Agency shall use the same degree of care but no less than a reasonable degree of care as Vendor/Agency uses to protect its own proprietary or confidential information of a like nature.

6. No copies may be made of the Confidential Information without the prior written consent of PERKESO and in the event approval is given, all confidential or proprietary legends or markings on the original must be retained on the copies.

7. The confidentiality obligations in this Agreement shall not apply to any information which (a) is or becomes publicly available to the public through no fault of the Vendor/Agency; (b) is rightfully received by Vendor/Agency from a third party without proprietary or confidential limitations; (c) is independently developed by Vendor/Agency without use of the Confidential Information; or (d) was known to Vendor/Agency before first receipt from PERKESO.

8. This Agreement will not apply to prevent Vendor/ Agency from disclosing Confidential Information to the extent

required by law or regulations, provided Vendor/Agency asserts the confidentiality of the Confidential Information to the body seeking disclosure and notifies PERKESO may contest the disclosure or seek a protective order.

9. PERKESO warrants that it has the right to disclose the Confidential Information. No other warranties are made and no responsibility or liability is or will be accepted by PERKESO in relation to the accuracy or completeness of the Confidential Information wherein Confidential Information is provided "as is". In no event shall PERKESO be liable for incidental, indirect, or consequential damages in relation to the Confidential Information.

10. Upon PERKESO's written request, the Vendor/Agency shall, at PERKESO's election, return, destroy, or delete all documents or media containing Confidential Information, including all copies and extracts. The Vendor/Agency shall also provide documentation certifying that the Confidential Information has been returned, destroyed, or deleted in accordance with PERKESO's request. For the avoidance of doubt, any Confidential Information retained under this Agreement shall remain subject to the terms of this Agreement.

11. No waiver of any provision of this Agreement shall be binding unless executed in writing by the party making the waiver. No waiver of any of the provisions of this Agreement shall be deemed, or shall constitute, a waiver of such provision on any other occasion, nor the waiver of any other provision, whether or not similar. No delay in the enforcement of any provision in this Agreement shall constitute a waiver of the right to enforce such provision in that or any other instance.

12. This Agreement does not create any agency or partnership relationship or exclusivity obligations.

13. This Agreement imposes no obligation on PERKESO to disclose Confidential Information and PERKESO has no obligation under this Agreement to continue any discussions, or to offer or purchase any product or service, or to take or refrain from taking any other action except as expressly set out in this Agreement. Nothing in this agreement shall prevent PERKESO from pursuing similar discussions or transactions with third parties .

14. This Agreement does not confer on the Vendor/Agency any intellectual property rights to or over the Confidential Information.

15. Vendor/Agency acknowledges that damage for improper disclosure of Confidential Information may be irreparable; therefore PERKESO is entitled to seek equitable relief, including injunction and preliminary injunction in addition to all other remedies.

16. Vendor/Agency shall comply to Polisi Keselamatan Maklumat Pertubuhan Keselamatan Sosial (PKM PERKESO) in regards to all ICT related project.

17. Vendor/Agency shall comply to the Personal Data Protection Act 2010 (Act 709) and must issue PERKESO their Code of Practice before receiving any Confidential Information.

18. The Vendor/Agency shall strictly comply with the Official Secrets Act 1972 (Act 88) provisions concerning the handling, storage, dissemination, and management of all Confidential Information disclosed, accessed or obtained in the course business relationship between the Parties for the Project / Services. Any breach of the Act in relation to the Confidential Information shall be deemed a material breach of this Agreement.

19. Any addition or modification to this Agreement must be made in writing and signed by both parties.

20. This Agreement is the full understanding of the Parties relative to the protection of Proprietary Information and supersedes all other understandings with respect thereto.

21. This Agreement is made under and shall be construed according to the laws of Malaysia.

Signed:-

PERTUBUHAN KESELAMATAN SOSIAL

.....

Name :
Title :
Date :

VENDOR / AGENCY/EMPLOYEE

.....

Name :
Title :
Date :

LAMPIRAN C

Clause on Cyber Security

Security Standards Compliance

[Party A/Party B] shall implement and maintain the highest standard of administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of data and systems from unauthorized access, disclosure, alteration, and destruction. The Parties agree to comply with all applicable laws and regulations concerning cybersecurity, data protection, and privacy including but not limited to the Cyber Security Act 2024, Personal Data Protection Act 2010 and Official Secrets Act 1972, and any other relevant local or international cybersecurity frameworks.

Cybersecurity Responsibilities

[Party A/Party B] shall take reasonable steps to protect its IT infrastructure, networks, applications, and systems from cyber threats, including malware, phishing, ransomware, and other forms of cyberattacks, including but not limited to—

(a) Regularly update and patch systems to mitigate vulnerabilities;
(b) Maintain an incident response plan to address cybersecurity breaches;
(c) Use encryption for the transmission and storage of sensitive data;
(d) Ensure that all personnel accessing the systems are properly trained on cybersecurity risks;
(e) Protection against unauthorized or unlawful access, disclosure, alteration, destruction, or accidental loss of data;
(f) Regular system updates, patching, and vulnerability management;
(g) Use of encryption to safeguard sensitive data in transit and storage; and
(h) *Implementation of firewalls, anti-virus, anti-malware, and other protective technologies.*

Data Breach Notification

In the event of a data breach or cybersecurity incident that compromises or may compromise the security of data and system under this Agreement, the affected Party shall:

(a) *Notify the other Party in writing without undue delay, but no later than [X] hours after discovering the breach;*
(b) *Provide detailed information regarding the nature of the breach, including the compromised data, the extent of the breach, and any actions taken to mitigate the risk; and*
(c) *Cooperate fully with the other Party to assist in investigating the breach, mitigating potential harm, and fulfilling any legal reporting requirements.*

Audit Rights

The Parties acknowledge that cybersecurity compliance may be subject to periodic audits to verify adherence to the cybersecurity standards outlined in this Agreement. Upon reasonable notice, [Party A/Party B] shall provide access to its systems, processes, and records necessary for the audit, and shall make available qualified personnel to respond to audit inquiries.

Third-Party Service Providers

In the event that [Party A/Party B] uses third-party vendors or service providers to process or store data, the Party must ensure that those third parties adhere to the same cybersecurity standards and obligations as outlined in this clause. Written agreements must be in place to ensure that the third-party providers comply with relevant data protection laws and maintain appropriate security measures.

Liability for Cybersecurity Failures

In the event of a data breach or cybersecurity incident caused by the negligence or failure of [Party A/Party B] to implement adequate security measures, the responsible Party shall be liable for all costs, damages, and losses incurred, including any penalties or fines imposed by regulatory authorities such as the Personal Data Protection Commissioner or National Cyber Security Agency.

LAMPIRAN D

Clause on Confidentiality

1. ***CONFIDENTIALITY***

1.1 Confidential Information

(a) Terms of clauses related to confidentiality, intellectual property and liability of this Agreement shall survive any termination of this Agreement.

(b) *For the purposes of this clause 'Confidential Information' means all information (whether commercial, financial, technical or otherwise) relating to the disclosing party, its sub-contractors and suppliers, disclosed to or otherwise obtained by the recipient party under or in connection with the Project and this Agreement and which is designated as being confidential or which is by its nature clearly confidential.*

1.2 Undertakings

Each Party undertakes in respect of Confidential Information for which it is the recipient -

(a) to treat such Confidential Information as confidential;

(b) not without the disclosing Party's prior approval to communicate or disclose any part of such Confidential Information to any person except:-

(i) only to those employees, agents, sub-contractors and other suppliers on a need to know basis who are directly involved with the Agreement; and

(ii) the recipient's auditors, professional advisers and any other persons or bodies having a legal right or duty to have access to or knowledge of the Confidential Information in connection with the business of the recipient;

(c) to ensure that all persons and bodies mentioned in Clause 1.2(b)(ii) are made aware, prior to disclosure of the confidential nature of the Confidential Information and that they owe a duty of confidence to the disclosing party and to use all reasonable endeavors to ensure that such persons and bodies comply with the provisions of this Clause;

(d) *not to use or circulate such Confidential Information within its own organization except to the extent necessary for the purposes of this Agreement;*

(e) *not to make public any information as to the recommendations, assessments and opinions formulated in the course of or as a result of the provision and performance of the Agreement;*

(f) *not to make or cause to be made any press statement or otherwise relating to the Confidential Information and the Agreement; and*

(g) *not to publish or course to be published any material whatsoever relating to the Confidential Information and the Agreement without the prior written approval of the other Party.*

1.3 Exceptions

The obligations in Clause 1.2 shall not apply to any Confidential Information -

(a) in the recipient's possession (with full right to disclose) before receiving it;
(b) which is or becomes public knowledge other than by breach of this Clause;

(c) is independently, developed by the recipient without access to or use of the Confidential Information;

(d) is lawfully received from a third party (with full right to disclose); or

(e) required to by law, where the receiving Party has notified the disclosing Party of the required disclosure, reasonably assists the disclosing Party (at the disclosing Party's cost) to obtain a protective order, and limits the disclosure to only that information, which in the opinion of receiving Party's, is required to fulfill the requirement.

1.4 Survival

This clause shall continue in force notwithstanding the termination or expiration of this Agreement for any reason.

LAMPIRAN E

RUJUKAN
SENARAI PERUNDANGAN DAN PERATURAN

Polisi Keselamatan Siber PERKESO ini hendaklah dibaca bersama dengan Akta-Akta, perundangan subsidiari, pekeliling-pekeliling, surat pekeliling dan arahan pentadbiran/peraturan dalaman yang berkaitan dan sedang berkuatkuasa antaranya seperti berikut:

1. Akta 854 - Akta Keselamatan Siber 2024 (26 Jun 2024)
2. Akta 709 - Akta Perlindungan Data Peribadi 2010
3. Akta Komunikasi dan Multimedia 1998
4. Akta Jenayah Komputer 1997
5. Akta Tandatangan Digital 1997
6. Akta Hak Cipta (Pindaan) Tahun 1997
7. Akta Rahsia Rasmi 1972
8. Akta 658 – Akta Perdagangan Elektronik 2006
9. Akta 629 - Akta Arkib Negara 2003
10. Akta 606 - Akta Cakera Optik 2000
11. Akta Keselamatan Sosial Pekerja 1969 [Akta 4]
12. Akta Jalan, Parit dan Bangunan 1974 (Akta 133)
13. Akta Perkhidmatan Bomba 1988 (Akta 341)
14. Akta Kilang & Jentera 1967 (Akta 139)
15. Electricity Regulation 1994
16. Akta 298 - Kawasan Larangan Tempat Larangan 1959
17. Akta 56 - Akta Keterangan 1950
18. *National Cyber Security Policy* (NCSP)
19. Perintah - Perintah Am
20. Perintah Am Bab D
21. Kaedah-Kaedah Keselamatan Sosial Pekerja (Kelakuan dan Tatatertib) 1994
22. Kaedah-Kaedah Keselamatan Sosial Pekerja (Jawatankuasa Tatatertib dan Lembaga Rayuan Tatatertib) 2001

23. Uniform Building By-Laws 1984 (UBBL)
24. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan pengendalian Insiden Keselamatan Siber Sektor Awam
25. Pekeliling Am Bilangan 2 Tahun 2021 - Manual Pengurusan Aset Menyeluruh Kerajaan versi 2.0
26. Pekeliling Am Bil. 1 Tahun 2015 - Pelaksanaan Data Terbuka Sektor Awam
27. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
28. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
29. Pekeliling Bilangan 8 Tahun 2024 – Garis Panduan Pengurusan Dan Pengendalian Rahsia Rasmi Dalam Perkhidmatan Awam
30. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam
31. Surat Pekeliling Am Bilangan 1 Tahun 2021 - Larangan Penggunaan Telefon Bimbit, Peralatan Eletronik yang Mampu Merakam Maklumat dalan Mesyuarat Penting Kerajaan
32. Surat Pekeliling Am Bilangan 1 Tahun 2009 Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan
33. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan. Penilaian Tahap Keselamatan Rangkaian Dan Sistem Ict. Sektor Awam
34. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan. Pengurusan Risiko Keselamatan Maklumat Sektor Awam
35. Arahan 20 (Semakan Semula) - Dasar dan Mekanisme Pengurusan Bencana Negara
36. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara
37. Arahan MKN No. 26 Pengurusan Keselamatan Siber Negara 21 Disember 2021
38. Arahan Keselamatan (Semakan dan Pindaan 2017)
39. Arahan Ketua Pegawai Keselamatan Kerajaan 5 Jun 2012 - Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam
40. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007)

41. Arahan Perbendaharaan
42. Arahan, Pekeliling, Garis Panduan dan Memo yang berkaitan perolehan PERKESO
43. Arahan Pentadbiran Tanggungjawab Bahagian Dan Pejabat Dalam Pembangunan, Penambahbaikan Dan Penyelenggaraan Sistem Aplikasi ICT Pertubuhan Keselamatan Sosial (PERKESO)
44. Surat Arahan Ketua Pengarah MAMPU - Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh: 8 April 2011)
45. Surat Arahan Ketua Pengarah MAMPU - Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan. (Tarikh: 1 Julai 2010)
46. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.
47. Surat Arahan Ketua Pengarah MAMPU 2010 - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam
48. Surat Arahan Ketua Pengarah MAMPU - Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam. (Tarikh: 4 Januari 2010)
49. Surat Arahan Ketua Pengarah MAMPU - Penggunaan Media Jaringan Sosial Di Sektor Awam. (Tarikh: 19 November 2009)
50. Surat Arahan Ketua Pengarah MAMPU - Penggunaan Smartphone, Personel Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh: 15 September 2009)
51. Surat Arahan Ketua Pengarah MAMPU 2007 - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007
52. Surat Arahan Ketua Pengarah MAMPU 2007 - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi - Agensi Kerajaan yang bertarikh 23 November 2007
53. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi - Agensi Kerajaan, 23 November 2007
54. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006

55. Garis Panduan Pengurusan Projek ICT PERKESO (GPP) (10 Februari 2022).
56. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010)
57. Garis Panduan IT *Outsourcing* (Oktober 2006)
58. Garis Panduan Keselamatan MAMPU 2004
59. Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam
60. *Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisations*
61. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara
62. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi
63. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam
64. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016
65. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002
66. Manual Perolehan PERKESO (MPP)

Disediakan dan disemak oleh
Koordinator dan Pentadbir Pasukan Keselamatan Siber PERKESO:

Bahagian / Jabatan

Bahagian Khidmat Pengurusan

Bahagian ICT

Bahagian Strategi dan Transformasi

Bahagian Audit dan Risiko

Bahagian Perundangan dan Pendakwaan

Bahagian Sumber Manusia

Bahagian Komunikasi dan Hal Ehwal Korporat

Bahagian Pencegahan, Perubatan & Pemulihan

Bahagian Perolehan

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PERKESO

Nama : .....

No. Kad Pengenalan : .....

No. Pekerja* : .....

Jawatan* : .....
(Tetap ☐ Kontrak ☐ Sambilan ☐)

Pejabat PERKESO/ Bahagian* : .....

Nama Syarikat : .....
(Untuk diisi oleh pekerja atau pengguna luar yang berurusan dengan PERKESO)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah menerima buku Polisi Keselamatan Siber PERKESO;

2. Saya memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber PERKESO; dan

3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya (seperti tindakan tatatertib atau surat tunjuk sebab) boleh diambil ke atas diri saya.

.....
(Tandatangan)

.....
(Cop Jabatan/Syarikat)

Tarikh: .....

Nota (*): Untuk diisi oleh anggota PERKESO sahaja

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PERKESO

Nama : .....

No. Kad Pengenalan : .....

No. Pekerja* : .....

Jawatan* : .....
(Tetap ☐ Kontrak ☐ Sambilan ☐)

Pejabat PERKESO/ Bahagian* : .....

Nama Syarikat : .....
(Untuk diisi oleh pekerja atau pengguna luar yang berurusan dengan PERKESO)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah menerima buku Polisi Keselamatan Siber PERKESO;

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

3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya (seperti tindakan tatatertib atau surat tunjuk sebab) boleh diambil ke atas diri saya.

.....
(Tandatangan)

.....
(Cop Jabatan/Syarikat)

Tarikh: .....

Nota (*): Untuk diisi oleh anggota PERKESO sahaja

VERSI 2.0

KEMENTERIAN SUMBER MANUSIA

PERKESO

Pertubuhan Keselamatan Sosial (PERKESO)
Kementerian Sumber Manusia
Tingkat 11 Menara PERKESO
281 Jalan Ampang
50538 Kuala Lumpur