TERHAD

VERSI 1.1

KEMENTERIAN SUMBER MANUSIA

PERKESO

POLISI KESELAMATAN SIBER (PKSB)

PERTUBUHAN KESELAMATAN SOSIAL

PENGGUNA LUAR

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

Versi 1.1

14 Disember 2022

INFORMASI DOKUMEN

VERSI	KELULUSAN	TARIKH KUATKUASA
Versi 1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) PERKESO Bil 3/2022	25 April 2022
Versi 1.1	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) PERKESO Bil 8/2022	13 Disember 2022

A. REKOD PINDAAN

Tarikh	VERSI	PINDAAN/PENAMBAHAN
14 Disember 2022	1.1	Pindaan Bidang 05(A.9) Kawalan Akses (*Access Control*), DP050403(A.9.4.3) Sistem Pengurusan Kata Laluan (*Password Management System*). Tambahbaik para c. Panjang kata laluan digalakkan mempunyai **LAPAN (8) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **KECUALI** kelulusan khas daripada CSIRT PERKESO. Pindaan Bidang 05(A.9) Kawalan Akses (*Access Control*), DP050205(A.9.2.5) Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*). Keluarkan penyataan "Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan".
14 Disember 2022	1.1	Pindaan Bidang 02(A.6) Perancangan Bagi Keselamatan Organisasi (*Organization of*

		Information Security). Tambahbaik sub bidang DP020101(A.6.1.1) Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and Responsibility of Information Security*), para (x) *Cyber Security Incident Response Team* (CSIRT PERKESO). Mengemaskini peranan dan tanggungjawab CSIRT PERKESO adalah seperti berikut : a. Memaklumkan insiden keselamatan siber kepada CSIRT PERKESO (sekiranya ada); dan b. Memantau, mengesan dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber; c. Melaksanakan pengurusan insiden keselamatan siber; dan d. Menyebarkan makluman/amaran berkaitan insiden keselamatan siber kepada semua warga PERKESO.
14 Disember 2022	1.1	Pindaan Bidang 02(A.6) Perancangan Bagi Keselamatan Organisasi (*Organization of Information Security*). Tambahbaik sub bidang DP020101(A.6.1.1) Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and Responsibility of Information Security*), para (xi) Pasukan Petugas Keselamatan Siber (PPKS) PERKESO. Peranan

		dan tanggungjawab PPKS adalah seperti berikut : a. Menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber; b. Bertindak sebagai *first level support* kepada CSIRT PERKESO dalam mengendalikan insiden keselamatan siber, mengawasi dan memberi khidmat nasihat berkaitan keselamatan siber; c. Merekod dan menjalankan siasatan awal terhadap insiden yang diterima; d. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; dan e. Menyediakan laporan insiden keselamatan siber.
14 Disember 2022	1.1	Mengemas kini pernyataan : "*Computer Emergency Response Team* (CERT)" kepada "*Cyber Security Incident Response Team* (CSIRT)"

Diluluskan Oleh:

Jawatankuasa Pemandu ICT (JPICT) PERKESO.

Bidang Polisi Keselamatan Siber PERKESO

Bidang 01(A.5) Polisi Keselamatan Maklumat
Bidang 02(A.6) Perancangan Bagi Keselamatan Maklumat
Bidang 03(A.7) Keselamatan Sumber Manusia
Bidang 04(A.8) Pengurusan Aset
Bidang 05(A.9) Kawalan Akses
Bidang 06(A.10) Kriptografi
Bidang 07(A.11) Keselamatan Fizikal dan Persekitaran
Bidang 08(A.12) Keselamatan Operasi
Bidang 09(A.13) Keselamatan Komunikasi
Bidang 10(A.14) Pemerolehan, Pembangunan dan Penyelenggaraan Sistem
Bidang 11(A.15) Hubungan Dengan Pembekal
Bidang 12(A.16) Pengurusan Insiden Keselamatan Maklumat
Bidang 13(A.17) Aspek Keselamatan Maklumat dalam Pengurusan Kesinambungan Perkhidmatan
Bidang 14(A.18) Pematuhan

Format Polisi Keselamatan Siber PERKESO

DP010101 (A.5.1.1) Polisi Keselamatan Maklumat

DP	01	01	01	A.5.1.1
PKSB PERKESO	Bidang	Objektif mengikut Bidang	Kawalan Objektif Bagi Objektif mengikut Bidang	Kod yang digunakan dalam ISO/IEC 27001:2013

PENGENALAN

Polisi Keselamatan Siber (PKSB) PERKESO ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh pengguna luar yang mempunyai urusan dengan perkhidmatan ICT PERKESO dalam melindungi maklumat di ruang siber.

ASET ICT PERKESO

Aset ICT PERKESO merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti berikut :

(1) Maklumat

Semua penyedia perkhidmatan dalam PERKESO hendaklah mengenal pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori :

(a) Maklumat Rahsia Rasmi

Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B Akta Rahsia Rasmi 1972.

(b) Maklumat Rasmi

Maklumat Rasmi ialah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh PERKESO semasa

menjalankan urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

(c) Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau *Personally Identifiable Information*) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

(2) Aliran Data

Aliran Data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran Data dan komunikasi dalam PERKESO hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk :

(a) Saluran komunikasi dan aliran data antara sistem di PERKESO;
(b) Saluran komunikasi dan aliran data ke sistem luar; dan
(c) Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan (*cloud computing*) dianggap sebagai saluran komunikasi luaran.

(3) Sistem Luaran

Sistem Luaran ialah sistem bukan milik PERKESO yang dihubungkan dengan sistem PERKESO. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

(4) Sumber Luaran

Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi PERKESO. Contoh perkhidmatan sumber luaran ialah :

(a) Perisian Sebagai Satu Perkhidmatan
(b) Platform Sebagai Satu Perkhidmatan
(c) Infrastruktur Sebagai Satu Perkhidmatan

(d) Storan Pengkomputeran Awan

(e) Pemantauan Keselamatan

Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

RISIKO

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

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya **sekali setahun** atau apabila berlaku sebarang perubahan ketara kepada persekitaran siber PERKESO.

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut :

(1) Penguraian Risiko

(a) Penguraian Risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

(b) Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut :

(i) Teknologi

Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk menghadkan capaian logikal kepada sistem tertentu.

(ii) Proses

Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

(iii) Manusia

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

(2) Pengurusan Risiko

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

(1) Mengenal pasti kerentanan;
(2) Mengenal pasti ancaman;
(3) Menilai risiko;
(4) Menentukan penguraian risiko;
(5) Memantau keberkesanan penguraian risiko; dan
(6) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

(b) Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** atau apabila perlu oleh Bahagian masing-masing dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ICT dan Jawatankuasa Pelaksana ISMS PERKESO.

TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut :

(1) Perlindungan Ketirisan Data

(a) Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

(b) Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

(2) Elemen Dalam Persekitaran Pengkomputeran

Maklumat Rahsia Rasmi hendaklah disimpan dan diproses dalam persekitaran pengkomputeran mengikut Arahan Keselamatan yang dikeluarkan oleh Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) atau mendapat pengesahan dari CGSO.

Setiap projek ICT yang dibangunkan di PERKESO hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi, kawalan keselamatan bagi setiap kategori elemen di bawah :

(a) Peranti Pengkomputeran Peribadi

(1) Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk beinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja, telefon pintar, tablet dan peranti storan.

(2) Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada PERKESO. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

MANUSIA

Pengguna Luar hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

(1) Kompetensi Pengguna

(a) Kompetensi pengguna termasuk kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

(b) Kompetesi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

(c) Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

(2) Peranan

(a) Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

(b) Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa depan.

(c) Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.

PERNYATAAN POLISI KESELAMATAN SIBER PERKESO

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan sistem ICT sentiasa beroperasi secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Pengguna Luar hendaklah mematuhi pernyataan polisi keselamatan siber PERKESO dan memaklumkan kepada PERKESO sekiranya terdapat apa-apa ancaman dan risiko berkaitan dengan perkara yang menjejaskan keselamatan siber PERKESO

Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rasmi organisasi mengikut klasifikasi dari capaian tanpa kuasa yang sah;
b. Menjamin setiap maklumat adalah tepat dan sempurna;
c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d. Memastikan akses kepada pengguna-pengguna yang sah.

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

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

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT PERKESO, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

14 bidang keselamatan yang terlibat di dalam Polisi Keselamatan Siber PERKESO diterangkan dengan lebih jelas dan teratur seperti berikut :

Bidang 01(A.5) Polisi Keselamatan Maklumat (*Information Security Policy*)

0101(A.5.1) Hala Tuju Pengurusan Untuk Keselamatan Maklumat (*Management Direction for Information Security*)

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PERKESO dan perundangan yang berkaitan.

DP010101(A.5.1.1) Polisi Keselamatan Maklumat (*Policies for Information Security*)

Polisi Keselamatan Siber PERKESO mestilah dipatuhi oleh semua pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP010102(A.5.1.2) Kajian Semula Polisi Untuk Keselamatan Maklumat (Review *of Policies for Information Security*)

Hanya terpakai untuk anggota PERKESO sahaja

Bidang 02(A.6) Perancangan Bagi Keselamatan Organisasi (*Organization of Information Security*)
0201(A.6.1) Perancangan Dalaman (*Internal Organization*)
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber PERKESO.
DP020101(A.6.1.1) Peranan dan Tanggungjawab Keselamatan Maklumat (*The Role and* Responsibility *of Information Security*)
Hanya terpakai untuk anggota PERKESO sahaja
DP020102(A.6.1.2) Anggota PERKESO
Hanya terpakai untuk anggota PERKESO sahaja
DP020103(A.6.1.3) Pengguna Luar

Peranan dan tanggungjawab anggota luar adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakanya; c. Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan d. Melaksanakan langkah-langkah perlindungan seperti berikut :	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

(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, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (v) Menjaga kerahsiaan kawalan keselamatan siber 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 Soalan Keselamatan (KPKK 11)**.	
DP020104(A.6.1.4) Pengasingan Tugas (*Segregation of Duties*)	
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja	
DP020105(A.6.1.5) Hubungan Dengan Pihak Berkuasa (*Contact with Authorities*)	
Hanya terpakai untuk anggota PERKESO sahaja	
DP020106(A.6.1.6) Hubungan Dengan Kumpulan Berkepentingan Yang Khusus (*Contact with Special Interest Groups*)	
Hanya terpakai untuk anggota PERKESO sahaja	
DP020107(A.6.1.7) Keselamatan Maklumat Dalam Pengurusan Projek (*Information Security in Project Management*)	
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja	

0202(A.6.2) Peranti Mudah Alih dan Telekerja

Objektif:

Memastikan keselamatan telekerja dan penggunaan peralatan mudah alih.

DP020201(A.6.2.1) Polisi Peranti Mudah Alih (*Mobile Device Policy*)

Hanya terpakai untuk anggota PERKESO sahaja

DP020202(A.6.2.2) Telekerja (*Teleworking*)

Hanya terpakai untuk anggota PERKESO sahaja

Bidang 03(A.7) Keselamatan Sumber Manusia (*Human Resource Security*)

0301(A.7.1) Sebelum Perkhidmatan (*Prior To Employment*)

Objektif:

Memastikan pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

DP030101(A.7.1.1) Tapisan Keselamatan (*Security Screening*)

Tapisan keselamatan hendaklah dijalankan terhadap pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP030102(A.7.1.2) Terma & Syarat Perkhidmatan (*Terms and Conditions of Employment*)	
Persetujuan berkontrak dengan pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti berikut : a. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO yang terlibat dalam menjamin keselamatan aset ICT; dan b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

0302(A.7.2) Dalam Tempoh Perkhidmatan (*During Deployment*)

Objektif:

Memastikan pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

DP030201(A.7.2.1) Tanggungjawab Pengurusan (*Manegement Responsibilities*)	
PERKESO hendaklah memastikan pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO
DP030202(A.7.2.2) Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (*Information Security Awareness, Education and Training*)	
Hanya terpakai untuk anggota PERKESO sahaja	
DP030203(A.7.2.3) Proses Tatatertib (*Disciplinary Process*)	
Hanya terpakai untuk anggota PERKESO sahaja	
0303(A.7.3) Penamatan atau Perubahan Perkhidmatan (*Termination and Change of Employment*)	
Objektif: Memastikan tamat perkhidmatan pengguna luar diurus dengan teratur .	
DP030301(A.7.3.1) Penamatan atau Pertukaran Tanggungjawab Perkhidmatan (*Termination or Change of Employment Responsibilities*)	
Pengguna Luar yang telah tamat perkhidmatan perlu mematuhi perkara-perkara berikut :	Pengguna Luar dan pihak yang mempunyai urusan dengan

a. Memastikan semua aset ICT dikembalikan kepada PERKESO mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan PERKESO dan/atau terma perkhidmatan yang ditetapkan; dan c. Maklumat rasmi PERKESO dalam peranti tidak dibenarkan dibawa keluar dari PERKESO.	perkhidmatan ICT PERKESO

Bidang 04(A.8) Pengurusan Aset (*Asset Management*)
0401(A.8.1) Tanggungjawab Terhadap Aset (*Responsibility for Assets*)
Objektif: Untuk mengenal pasti aset bagi memberikan dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PERKESO.
DP040101(A.8.1.1) Inventori Aset (*Inventory of Asset*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040102(A.8.1.2) Pemilikan Aset (*Ownership of Assets*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040103(A.8.1.3) Penggunaan Aset Yang Dibenarkan (*Acceptable Use of Assets*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040104(A.8.1.4) Pemulangan Aset (*Return of Assets*)
Hanya terpakai untuk anggota PERKESO sahaja
0402(A.8.2) Klasifikasi Maklumat (*Information Classification*)
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.
DP040201(A.8.2.1) Pengelasan Maklumat (*Classification of Information*)
Hanya terpakai untuk anggota PERKESO sahaja

DP040202(A.8.2.2) Pelabelan Maklumat (*Labelling of Information*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040203(A.8.2.3) Pengendalian Aset (*Handling of Assets*)
Hanya terpakai untuk anggota PERKESO sahaja
0403(A.8.3) Pengendalian Media (*Media Handling*)
Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.
DP040301(A.8.3.1) Pengurusan Media Mudah Alih (*Management of Removal Media*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040302(A.8.3.2) Pelupusan Media (*Disposal of Media*)
Hanya terpakai untuk anggota PERKESO sahaja
DP040303(A.8.3.3) Pemindahan Media Fizikal (*Physical Media Transfer*)
Hanya terpakai untuk anggota PERKESO sahaja

Bidang 05(A.9) Kawalan Akses (*Access Control*)

0501(A.9.1) Keperluan Kawalan Akses (*Requirement of Access Control*)

Objektif :

Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.

DP050101(A.9.1.1) Polisi Kawalan Akses (*Access Control Policy*)

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi; b. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e. Pengasingan peranan kawalan capaian; f. Kebenaran rasmi permintaan akses; g. Keperluan semakan hak akses berkala; h. Pembatalan hak akses;	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

i. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan j. Keistimewaan capaian.	

DP050102(A.9.1.2) Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian (*Access to Network and Network Services*)

Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari PERKESO. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian PERKESO, rangkaian agensi lain dan rangkaian awam; b. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

0502(A.9.2) Pengurusan Akses Pengguna (*User Access Management*)

Objektif:

Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kinidan menyokong dasar kawalan capaian pengguna sedia ada.

DP050201(A.9.2.1) Pendaftaran dan Pembatalan Pengguna (*User Registration and De-Registration*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050202(A.9.2.2) Peruntukan Akses Pengguna (User Access *Provisioning*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050203(A.9.2.3) Pengurusan Hak Akses Istimewa (*Management of Priviledge Access Rights)*
Hanya terpakai untuk anggota PERKESO sahaja
DP050204(A.9.2.4) Pengurusan Maklumat Pengesahan Rahsia Pengguna (*Management of Secret Authentication Information of Users*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050205(A.9.2.5) Kajian Semula Hak Akses Pengguna (*Review of User Access Rights*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050206(A.9.2.6) Pembatalan atau Pelarasan Hak Akses (*Removal or Adjustment of Access Rights*)
Hanya terpakai untuk anggota PERKESO sahaja
0503(A.9.3) Tanggungjawab Pengguna (*User Responsibilities*)
Objektif : Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.
DP050301(A.9.3.1) Penggunaan Maklumat Pengesahan Rahsia (*Use of Secret Authentication Information*)

Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti. Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber PERKESO; b. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakanya; c. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat PERKESO; d. Melaksanakan langkah-langkah perlindungan seperti berikut : i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia 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. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. e. Melaporkan sebarang aktiviti yang mengancam kesealamatan siber kepada ICTSO dengan segera; dan	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

f. Menghadiri program-program kesedaran mengenai keselamatan siber. Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti.	
0504(A.9.4) Kawalan Akses Sistem dan Aplikasi (*System and Application Access Control*)	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi.	
DP050401(A.9.4.1) Sekatan Akses Maklumat (*Information Access Restriction*)	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO
DP050402(A.9.4.2) Prosedur Log Masuk Yang Selamat (*Secure Log-on Procedure*)	
Hanya terpakai untuk anggota PERKESO sahaja	

DP050403(A.9.4.3) Sistem Pengurusan Kata Laluan (*Password Management System*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050404(A.9.4.4) Penggunaan Program Utiliti Yang Mempunyai Hak Istimewa (*Use of Privileged Utility Programs*)
Hanya terpakai untuk anggota PERKESO sahaja
DP050405(A.9.4.5) Kawalan Akses Kepada Kod Sumber Program (*Access Control to Program Source Code*)
Hanya terpakai untuk anggota PERKESO sahaja

Bidang 06(A.10) Kriptografi (*Cryptography*)

0601(A.10.1) Kawalan Kriptografi (*Cryptography Control)*

Objektif:

Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat.

DP060101(A.10.1.1) Polisi Penggunaan Kawalan Kriptografi (*Policy on the use of Cryptographic Control*)

Hanya terpakai untuk anggota PERKESO sahaja

DP060102(A.10.1.2) Pengurusan Kunci Awam *(Public Key Management*)

Hanya terpakai untuk anggota PERKESO sahaja

Bidang 07(A.11) Keselamatan Fizikal dan Persekitaran (*Physical and Environmental Security*)

0701(A.11.1) Kawasan Selamat (*Secure Areas*)

Objektif :

Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat PERKESO.

DP070101(A.11.1.1) Perimeter Keselamatan Fizikal (*Physical Security Parameter*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070102(A.11.1.2) Kawalan Kemasukan Fizikal (*Physical Entry Controls*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070103(A.11.1.3) Kawalan Pejabat, Bilik dan Kemudahan (*Securing Offices, Rooms and Facilities*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070104(A.11.1.4) Perlindungan Daripada Ancaman Luar dan Persekitaran (*Protecting Against External and Internal Environmental Threats*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070105(A.11.1.5) Bekerja di Kawasan Selamat (*Working In Secure Area*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070106(A.11.1.6) Kawasan Penyerahan dan Pemunggahan (*Delivery and Loading Area*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
0702(A.11.2) Peralatan ICT (*ICT Equipment*)
Objektif : Melindungi peralatan ICT PERKESO daripada kehilangan, kerosakan, kecurian dan disalahgunakan.
DP070201(A.11.2.1) Penempatan dan Perlindungan Peralatan ICT (*Equipment Siting and Protection*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP070202(A.11.2.2) Utiliti Sokongan (*Supporting Utilities*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP070203(A.11.2.3) Keselamatan Kabel (*Cabling Security*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP070204(A.11.2.4) Penyelenggaraan Peralatan (*Equipment Maintenance*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP070205(A.11.2.5) Pengalihan Aset (*Removal of Assets*)
Hanya terpakai untuk anggota PERKESO sahaja
DP070206(A.11.2.6) Keselamatan Peralatan dan Aset di Luar Premis (*Security of Equipment off-Premises*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP070207(A.11.2.7) Pelupusan Yang Selamat atau Penggunaan Semula Peralatan (*Secure Disposal or Re-Use of Equipment*)
Hanya terpakai untuk anggota PERKESO sahaja
DP070208(A.11.2.8) Peralatan Pengguna Tanpa Kawalan *(Unattended User Equipment*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP070209(A.11.2.9) Dasar Meja Kosong dan Skrin Kosong (*Clear Desk and Clear Screen Policy)*
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

Bidang 08(A.12) Keselamatan Operasi (*Operations Security*)
0801(A.12.1) Prosedur dan Tanggungjawab Operasi (*Operational Procedures and Responsibilities*)
Objektif : Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.
DP080101(A.12.1.1) Prosedur Operasi Yang Didokumenkan (*Documented Operating Procedures*)
Hanya terpakai untuk anggota PERKESO sahaja
DP080102(A.12.1.2) Pengurusan Perubahan (*Change Management*)
Hanya terpakai untuk anggota PERKESO sahaja
DP080103(A.12.1.3) Pengurusan Kapasiti (*Capacity Management*)
Hanya terpakai untuk anggota PERKESO sahaja
DP080104(A.12.1.4) Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (*Separation of Development, Test and Operational Facilities*)
Hanya terpakai untuk anggota PERKESO sahaja
0802(A.12.2) Perlindungan Daripada Perisian Hasad (*Protection From Malware*)
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.

DP080201(A.12.2.1) Kawalan *Daripada* Perisian Hasad (*Controls Against Malware*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
0803(A.12.3) Sandaran (*Backup*)
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.
DP080301(A.12.3.1) Sandaran Maklumat (*Information Backup*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
0804(A.12.4) Pengelogan dan Pemantauan (*Logging and Monitoring*)
Objektif: Merekodkan peristiwa dan menghasilkan bukti.
DP080401(A.12.4.1) Pengelogan Kejadian (*Event Logging*)
Hanya terpakai untuk anggota PERKESO sahaja
DP080402(A.12.4.2) Perlindungan Maklumat Log (*Protection of Log Information*)
Hanya terpakai untuk anggota PERKESO sahaja
DP080403(A.12.4.3) Log Pentadbir dan Pengendali (*Administrator and Operator Logs*)
Hanya terpakai untuk anggota PERKESO sahaja

DP080404(A.12.4.4) Penyeragaman Jam (*Clock Synchronisation)*
Hanya terpakai untuk anggota PERKESO sahaja
0805(A.12.5) Kawalan Perisian Yang Beroperasi (*Control of Operational Software*)
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.
DP080501(A.12.5.1) Pemasangan Perisian Pada Sistem Yang Beroperasi (*Installation of Software on Operational Systems*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
0806(A.12.6) Pengurusan Kerentanan Teknikal (*Technical Vulnerability Management*)
Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.
DP080601(A.12.6.1) Pengurusan Kerentanan Teknikal (*Management of Technical Vulnerabilities*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP080602(A.12.6.2) Sekatan ke atas Pemasangan Perisian (*Restriction on Software Installation*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

0807(A.12.7) Pertimbangan Tentang Audit Sistem Maklumat (*Information Systems Audit Considerations*)

Objektif:

Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

DP080701(A.12.7.1) Kawalan Audit Sistem Maklumat (*Information Systems Audit Controls*)

Hanya terpakai untuk anggota PERKESO sahaja

Bidang 09(A.13) Keselamatan Komunikasi (*Communications Security*)
0901(A.13.1) Pengurusan Keselamatan Rangkaian (*Network Security Management*)
Objektif: Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.
DP090101(A.13.1.1) Kawalan Rangkaian (*Network Control*)
Hanya terpakai untuk anggota PERKESO sahaja
DP090102(A.13.1.2) Keselamatan Perkhidmatan Rangkaian (*Security of Network Services*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP090103(A.13.1.3) Pengasingan Dalam Rangkaian (*Segregation in Networks*)
Hanya terpakai untuk anggota PERKESO sahaja
0902(A.13.2) Pemindahan Data dan Maklumat (*Information Transfer*)
Objektif: Memastikan keselamatan perpindahan / pertukaran data maklumat dan perisian antara PERKESO dan pihak luar terjamin.
DP090201(A.13.2.1) Polisi dan Prosedur Pemindahan Data dan Maklumat (*Information Transfer policies and Procedures*)

Perkara yang perlu dipatuhi adalah seperti yang berikut:	Pengguna Luar dan pihak

a. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah dipatuhi untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b. Terma pemindahan data, maklumat dan perisian antara PERKESO dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c. Media yang mengandungi maklumat perlu dilindungi; dan d. Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP090202(A.13.2.2) Perjanjian Mengenai Pemindahan Data dan Maklumat (*Agreement on Information Transfer*)

PERKESO perlu mengambil kira keselamatan maklumat organisasi dengan menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara PERKESO dengan pihak luar. Perkara yang perlu dipatuhi ialah: a . Ketua Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat PERKESO; b . Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat PERKESO; c . Mengenal pasti pihak yang bertangungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

d . PERKESO hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	
DP090203(A.13.2.3) Pesanan Elektronik (*Electronic Messaging*)	
Hanya terpakai untuk anggota PERKESO sahaja	
DP090204(A.13.2.4) Perjanjian Kerahsiaan atau Ketakdedahan (*Confidentiality and Non-Disclosure Agreement*)	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan didokumentasikan. Pengguna Luar hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang ditetapkan oleh PERKESO.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

Bidang 10(A.14) Pemerolehan, Pembangunan Dan Penyelenggaraan Sistem (*System Acquisition, Development and Maintenance*)

1001(A.14.1) Keperluan Keselamatan Sistem Maklumat (*Security Requirements of Information System*)

Objektif:

Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang seluruh kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan dalam rangkaian awam.

DP100101(A.14.1.1) Analisa dan Spesifikasi Keperluan Keselamatan Maklumat (*Information Security Requirements Analysis and Spesifications*)

Hanya terpakai untuk anggota PERKESO sahaja

DP100102(A.14.1.2) Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam (*Securing Application Services on Public Networks*)

Hanya terpakai untuk anggota PERKESO sahaja

DP100103(A.14.1.3) Melindungi Transaksi Perkhidmatan Aplikasi (*Protecting Application Services Transactions*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

1002(A.14.2) Keselamatan Dalam Proses Pembangunan dan Sokongan (*Security in Development and Support Services*)
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.
DP100201(A.14.2.1) Dasar Pembangunan Selamat (Secure Development Policy)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP100202(A.14.2.2) Prosedur Kawalan Perubahan Sistem (*System Change Control Procedures*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP100203(A.14.2.3) Kajian Semula Teknikal Bagi Aplikasi Selepas Perubahan Platform Operasi (*Technical Review of Applications after Operating Platform Changes*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP100204(A.14.2.4) Sekatan Ke Atas Perubahan Dalam Pakej Perisian (*Restrictrictions on Changes to Software Packages*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP100205(A.14.2.5) Prinsip Kejuruteraan Sistem Yang Selamat (*Secure System Engineering Principles*)
Hanya terpakai untuk anggota PERKESO sahaja

DP100206(A.14.2.6) Persekitaran Pembangunan Selamat (*Secure Development Environment*)
Hanya terpakai untuk anggota PERKESO sahaja
DP100207(A.14.2.7) Pembangunan Oleh Khidmat Luaran (*Outsourced Software Development*)
Hanya terpakai untuk anggota PERKESO sahaja
DP100208(A.14.2.8) Pengujian Keselamatan Sistem (*System Security Testing*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP100209(A.14.2.9) Pengujian Penerimaan Sistem (*System Accepting Testing*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
1003(A.14.3) Data Ujian (*Test Data*)
Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.
DP100301(A.14.3.1) Perlindungan Data Ujian (*Protection of Test Data*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

Bidang 11(A.15) Hubungan Pembekal (*Supplier Relationship*)
1101(A.15.1) Keselamatan Maklumat Dalam Hubungan Pembekal (*Information Security in Supplier Relationships*)
Objektif: Memastikan aset ICT PERKESO yang boleh dicapai oleh pembekal dilindungi.
DP110101(A.15.1.1) Polisi Keselamatan Maklumat Untuk Hubungan Pembekal (*Information Security Policy for Supplier Relationships*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP110102(A.15.1.2) Menangani Keselamatan Dalam Perjanjian Pembekal (*Addressing Security within Supplier Agreements*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
DP110103(A.15.1.3) Rantaian Bekalan Teknologi Maklumat dan Komunikasi (*Information and Communication Technology Supply Chain*)
Hanya terpakai untuk anggota PERKESO dan pembekal sahaja
1102(A.15.2) Pengurusan Penyampaian Perkhidmatan Pembekal (*Supplier Service Delivery Management*)
Objektif: Untuk mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.
DP110201(A.15.2.1) Memantau dan Mengkaji Semula Perkhidmatan Pembekal (*Monitoring and Review Supplier Services*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP110202(A.15.2.2) Menguruskan Perubahan Kepada Perkhidmatan Pembekal (*Managing Changes to Supplier Services*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

Bidang 12(A.16) Pengurusan Insiden Keselamatan Maklumat (*Information Security Incident Management*)
1201(A.16.1) Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan (*Management of Information Security Incidents and Improvements*)
Objektif: Memastikan pendekatan yang konsisten dan berkesan bagi pengurusan insiden keselamatan maklumat termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.
DP120101(A.16.1.1) Tanggungjawab dan Prosedur (*Responsibilities and Procedures*)
Hanya terpakai untuk anggota PERKESO sahaja
DP120102(A.16.1.2) Pelaporan Kejadian Keselamatan Maklumat (*Reporting Information Security Events*)
Hanya terpakai untuk anggota PERKESO sahaja
DP120103(A.16.1.3) Pelaporan Kelemahan Keselamatan Maklumat (*Reporting Security Weaknesses*)

Pengguna Luar yang menggunakan sistem dan perkhidmatan maklumat PERKESO dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP120104(A.16.1.4) Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat (*Assessment of and Decision Information Security Events*)
Hanya terpakai untuk anggota PERKESO sahaja
DP120105(A.16.1.5) Tindak Balas Terhadap Insiden Keselamatan Maklumat (*Response to Information Security Incidents*)
Hanya terpakai untuk anggota PERKESO sahaja
DP120106(A.16.1.6) Pembelajaran Daripada Insiden Keselamatan Maklumat (*Learning from Information Security Incidents*)
Hanya terpakai untuk anggota PERKESO sahaja
DP120107(A.16.1.7) Pengumpulan Bahan Bukti (*Collection of Evidence*)
Hanya terpakai untuk anggota PERKESO sahaja

Bidang 13(A.17) Aspek Keselamatan Maklumat Bagi Pengurusan Kesinambungan Perkhidmatan (*Information Security Aspects of Business Continuity Management*)

1301(A.17.1) Kesinambungan Keselamatan Maklumat (*Information Security Continuity*)

Objektif:
Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perniagaan PERKESO.

DP130101(A.17.1.1) Perancangan Kesinambungan Keselamatan Maklumat (*Planning Information Security Continuity*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP130102(A.17.1.2) Pelaksanaan Kesinambungan Keselamatan Maklumat (*Implementing Information Security Continuity*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

DP130103(A.17.1.3) Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat (*Verify, Review and Evaluate Information Security Continuity*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

1302(A.17.2) Lewahan (*Redundancy*)

Objektif:
Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

DP130201(A.17.2.1) Ketersediaan Kemudahan Pemprosesan Maklumat (*Availability of Information Prosecess Facilities*)

Hanya terpakai untuk anggota PERKESO dan pembekal sahaja

Bidang 14(A.18) Pematuhan (*Compliance*)

1401(A.18.1) Pematuhan Terhadap Keperluan Perundangan dan Kontrak (*Compliance with Legal and Contractual Requirements*)

Objektif:

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

DP140101(A.18.1.1) Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai (*Identification of Applicable Legislation and Contractual Agreement*)

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh pengguna luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP140102(A.18.1.2) Hak Harta Intelek (*Intellectual Property Rights*)

Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO

DP140103(A.18.1.3) Perlindungan Rekod (*Protection of Records*)	
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO
DP140104(A.18.1.4) Privasi dan Perlindungan Maklumat Peribadi (*Privacy and Protection of Personally Identifiable Information*)	
Pengguna Luar hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti yang tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Pengguna Luar dan pihak yang mempunyai urusan dengan perkhidmatan ICT PERKESO
DP140105(A.18.1.5) Peraturan Kawalan Kriptografi (Regulation of Cryptographic Controls)	
Hanya terpakai untuk anggota PERKESO sahaja	

1402(A.18.2) Kajian Semula Keselamatan Maklumat (*Information Security Reviews*)
Objektif: Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur PERKESO.
DP140201(A.18.2.1) Kajian Semula Keselamatan Maklumat Secara Berkecuali (*Independent Review of Information Security*)
Hanya terpakai untuk anggota PERKESO sahaja
DP140202(A.18.2.2) Pematuhan Polisi dan Standard Keselamatan (*Compliance with Security Policies and Standards*)
Hanya terpakai untuk anggota PERKESO sahaja
DP140203(A.18.2.3) Kajian Semula Pematuhan Teknikal (*Technical Compliance Review*)
Hanya terpakai untuk anggota PERKESO sahaja

GLOSARI	
Pengguna Luar	Terdiri daripada pelanggan dan pihak-pihak yang berkepentingan.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Aset Alih	Aset alih bermaksud aset yang boleh dipindahkan dari satu tempay ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan
Backup (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat.
Baki Risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan maklumat bagi menyokong arah tuju sesebuah organisasi.
Data-at-rest (data-dalam-simpanan)	*Refers to data that is being stored in stable destination systems. Data at rest is frequently defined as data that is not in use or is not travelling to system endpoints, such as mobile devices or workstations.*
Data-in-motion (data-dalam-pergerakan)	*Refers to a stream of data moving through any kind of network. It represents data which is being transferred or move.*
Data-in-use (data-dalam-penggunaan)	*Refers to data that is not simply being passively stored in a stable destination, such as a central data warehouse, but is working its way through other parts of an IT architecture.*
Defence-in-depth	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
ICT	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
ISMS	Information Security Management System Sistem Pengurusan Keselamatan Maklumat
PERKESO	Pertubuhan Keselamatan Sosial
Kerentanan	Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan
Kriptografi	Keadaan untuk menukar data dan maklumat biasa (standard format) kepada format yang tidak boleh difahami bagi melindungi penghantaran data dan maklumat
Lock	Mengunci komputer.
Mobile Code	Mobile Code merupakan suatu perisian yang boleh dipindahkan di antara sistem komputer dan rangkaian serta dilaksanakan tanpa perlu melalui sebarang proses pemasangan sebagai contoh Java Applet, ActiveX dan sebagainya pada pelayar internet.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Pengolahan risiko	Merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Ruang siber	Sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem tersebut secara fizikal atau maya serta persekitaran fizikal sistem-sistem tersebut dan semua aset yang berkaitan dengan ICT.
Server	Pelayan komputer
Source Code	Kod Sumber atau kod program (biasanya hanya dipanggil sumber atau kod) merujuk kepada sebarang siri pernyataan yang tertulis dalam bahasa pengaturcaraan komputer yang difahami manusia.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible PowerSupply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

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

Bahagian / Cawangan

Bahagian Strategi dan Transformasi

Bahagian Governan, Etika, Audit dan Risiko (GEAR)

Bahagian Perundangan

Bahagian Sumber Manusia

Bahagian Komunikasi Strategik

Bahagian Pencegahan, Perubatan & Pemulihan

Bahagian Perolehan

Bahagian Khidmat Pengurusan

Cawangan Pengurusan Hartanah

PERKESO

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PERKESO

Nama : .....

No. Kad Pengenalan : .....

No. Pekerja* : .....

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

Nama Pengguna / Agensi : .....
(Untuk diisi oleh pengguna luar atau Agensi 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

PERKESO

SURAT AKUAN PEMATUHAN
POLISI KESELAMATAN SIBER PERKESO

Nama : .....

No. Kad Pengenalan : .....

No. Pekerja* : .....

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

Nama Pengguna / Agensi : .....
(Untuk diisi oleh pengguna luar atau Agensi yang berurusan dengan PERKESO)

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

2. 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 1.1

KEMENTERIAN SUMBER MANUSIA

PERKESO

Pertubuhan Keselamatan Sosial (PERKESO)
Kementerian Sumber Manusia
Tingkat 16 Menara PERKESO
281 Jalan Ampang
50538 Kuala Lumpur