SURUHANJAYA KOPERASI Malaysia

DASAR KESELAMATAN ICT (DKICT)

SURUHANJAYA KOPERASI MALAYSIA

DISEMBER 2023 VERSI 1.1

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
09 MEI 2023	1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Suruhanjaya Koperasi Malaysia Bilangan 2/2023 Mesyuarat Lembaga Pengarah Suruhanjaya Koperasi Malaysia Bilangan 5/2023	12 Mei 2023 29 September 2023
15 DISEMBER 2023	1.1	Bengkel Pemurnian Dokumen Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (DKICT 1.0)	12 Dis - 13 Dis 2023

ISI KANDUNGAN

SURUHANJAYA KOPERASI MALAYSIA

ISI KANDUNGAN

PENGENALAN

SURUHANJAYA KOPERASI MALAYSIA

PENGENALAN

Dasar Keselamatan ICT (DKICT) Suruhanjaya Koperasi Malaysia (SKM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada pegawai SKM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT SKM. Dasar Keselamatan ICT SKM diwujudkan berdasarkan Pelan Pendigitalan SKM 2021-2025 (Teras Strategik 3.3 – Membangunkan Dasar Keselamatan ICT / Dasar Perkongsian Data Serta Garis Panduan Yang Berkaitan). DKICT SKM menggunapakai DKICT Kementerian Pembangunan Usahawan dan Koperasi (KUSKOP) 2.0, DKICT Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) 5.3 dan Jabatan Perkhidmatan Awam (JPA) 2.6 sebagai rujukan utama.

Maklumat rahsia rasmi dan maklumat rasmi SKM hendaklah selaras dengan Akta Rahsia Rasmi 1972 [Akta 88], Akta Perlindungan Data Peribadi 2010 [Akta 709], peraturan-peraturan, garis panduan dan pekeliling-pekeliling yang dikeluarkan oleh pihak MAMPU.

OBJEKTIF DASAR KESELAMATAN ICT SKM

SURUHANJAYA KOPERASI MALAYSIA

OBJEKTIF DASAR KESELAMATAN ICT SKM

Dasar Keselamatan ICT SKM diwujudkan untuk menjamin kesinambungan urusan SKM dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi SKM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT SKM ialah seperti berikut:

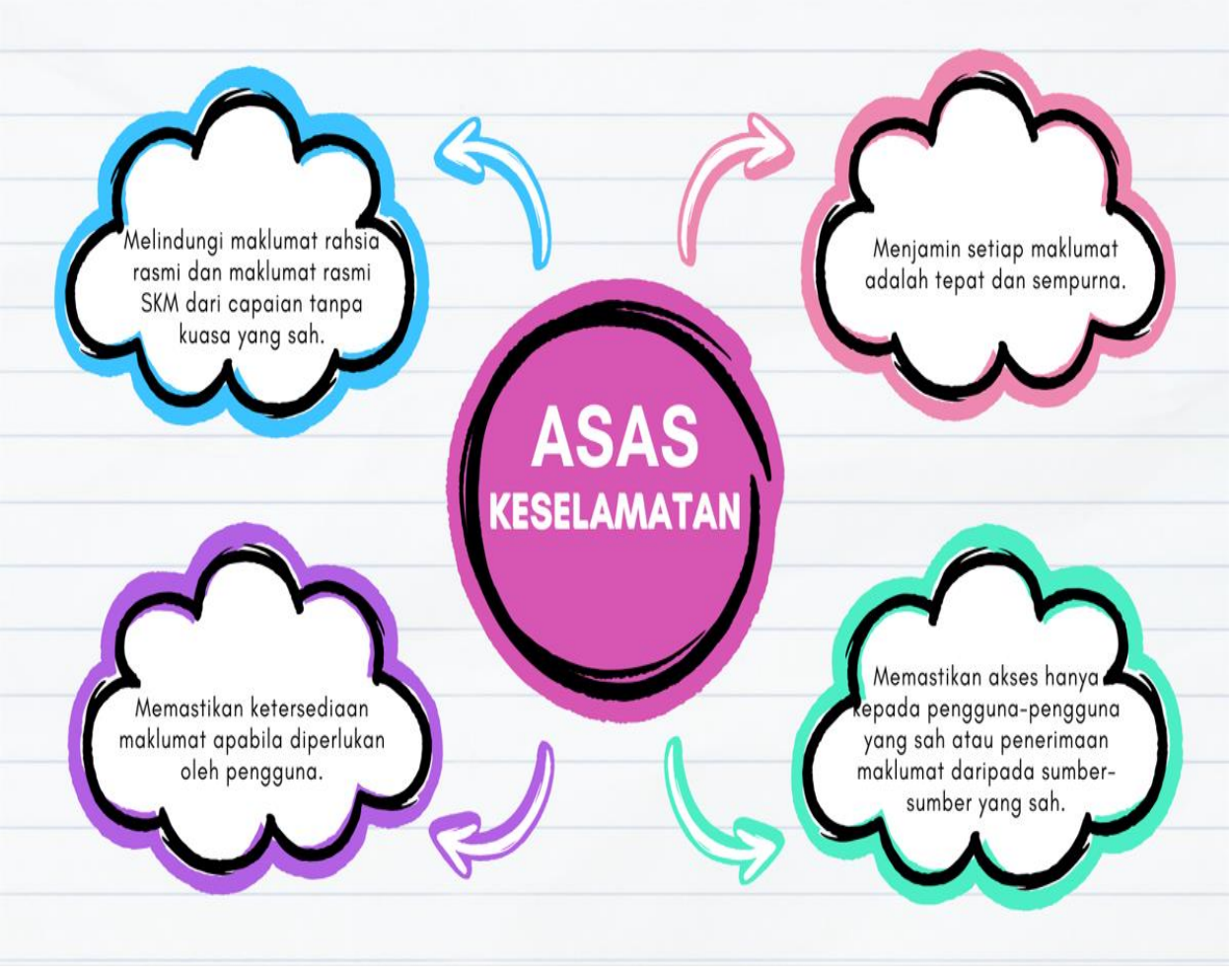
PERNYATAAN DASAR KESELAMATAN ICT SKM

SURUHANJAYA KOPERASI MALAYSIA

PERNYATAAN DASAR KESELAMATAN ICT SKM

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

Keselamatan ICT adalah bermaksud keadaan bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat (4) komponen asas keselamatan ICT, iaitu:



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

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

SKOP DASAR KESELAMATAN ICT SKM

SURUHANJAYA KOPERASI MALAYSIA

SKOP DASAR KESELAMATAN ICT SKM

Sistem ICT SKM terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT, data dan maklumat. SKM telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

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

2. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan SKM.

Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, DKICT SKM ini merangkumi perlindungan ke atas semua bentuk maklumat ICT kerajaan yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan yang dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

1. Data dan maklumat

   Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT.

2. Peralatan ICT

   Semua peralatan komputer dan *peripheral* seperti *server*, *firewall*, komputer peribadi, stesen kerja, kerangka utama, pencetak, peralatan multimedia dan alat-alat prasarana seperti *Uninterruptible Power Supply* (UPS), punca kuasa dan lain-lain.

3. Media storan

Semua media storan yang digunakan untuk menyimpan data dan maklumat seperti *optical disk*, *flash disk*, *hard disk*, USB *flash drive*, *cartridge tape*, *compact disc* (CD) dan lain-lain.

4. Media komunikasi

Semua peralatan berkaitan komunikasi seperti pelayan atau perkakasan rangkaian, *gateway*, *router*, peralatan PABX, *wireless* LAN, talian Metro-E, peralatan *video conferencing*, modem, kabel rangkaian, NIC, *switches* dan sebagainya.

5. Perisian

Semua jenis perisian yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data atau maklumat. Ini termasuklah sistem aplikasi seperti SAGA - SKM *Financial System*, Infokop, Aplikasi *Online* dan perisian sistem seperti Windows, LINUX serta perisian utiliti, perisian komunikasi, sistem pengurusan pangkalan data, fail program, fail data dan lain-lain.

6. Dokumentasi

Semua dokumen termasuk prosedur dan manual pengguna yang berkaitan dengan aset ICT, dokumen pemasangan dan pengoperasian peralatan dan perisian.

7. Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang diguna untuk menempatkan perkara 1 hingga 6 di atas.

8. Manusia

   Semua pengguna yang dibenarkan.

9. Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsinya. Contoh:

   i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
   ii. Sistem halangan akses seperti sistem kad akses; dan
   iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

PRINSIP-PRINSIP DASAR KESELAMATAN ICT SKM

SURUHANJAYA KOPERASI MALAYSIA

PRINSIP-PRINSIP DASAR KESELAMATAN ICT SKM

Akses Atas Dasar Perlu Mengetahui

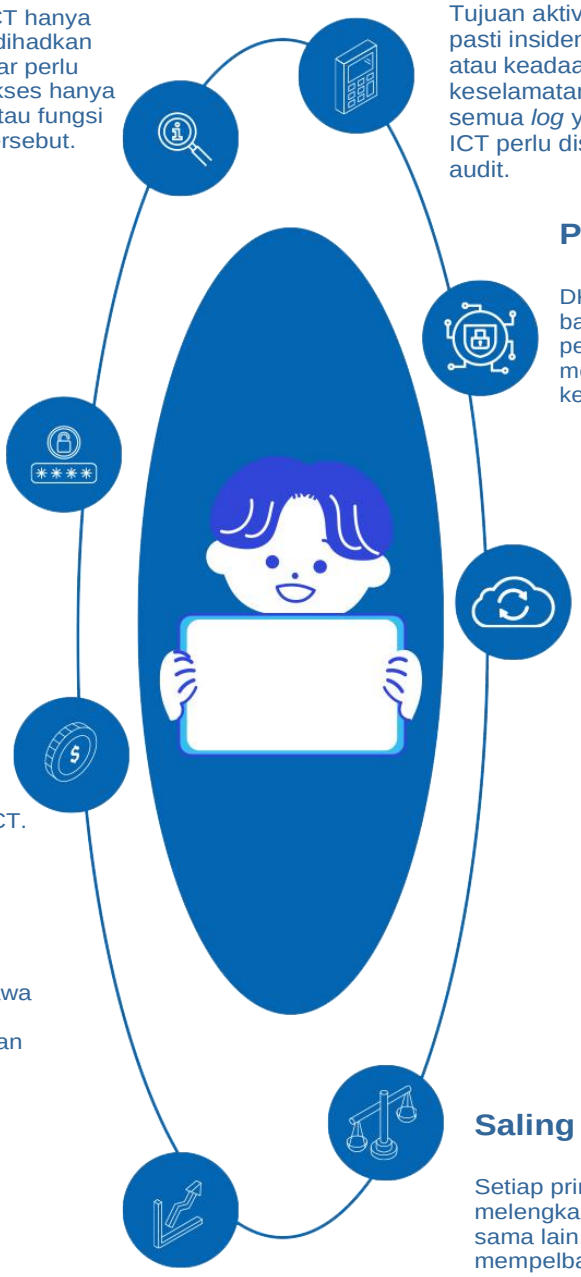
Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

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 dan menghapuskan sesuatu data atau maklumat.

Kebertanggungjawaban atau Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Bagi menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesahkan bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.



Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan aset ICT atau keadaan yang mengancam keselamatan aset ICT. Dengan itu, semua *log* yang berkaitan dengan aset ICT perlu disimpan bagi tujuan jejak audit.

Pematuhan

DKICT SKM hendaklah dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian bagi meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan dan ketidakbolehcapaian. Pemulihan boleh dilakukan melalui proses sandaran (*backup*) dan mewujudkan Pelan Pemulihan Bencana (DRP) di bawah Pengurusan Kesinambungan Perkhidmatan (PKP).

Saling bergantung

Setiap prinsip adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksimum.

Pengasing

Tugas mewujud, menghapus, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan (*unauthorized access*) serta melindungi aset ICT daripada kesilapan kebocoran maklumat terperingkat atau dimanipulasikan, pengasingan merangkumi data, operasi, pangkalan data dan rangkaian.

PENILAIAN RISIKO KESELAMATAN ICT

SURUHANJAYA KOPERASI MALAYSIA

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat SKM termasuklah aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses dan prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

SKM bertanggungjawab melaksana dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

SKM perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

2. Menerima atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;

3. Mengelak atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak atau mencegah berlakunya risiko; dan

4. Memindahkan risiko kepada pihak luaran yang berkepentingan.

TADBIR URUS KESELAMATAN MAKLUMAT

SURUHANJAYA KOPERASI MALAYSIA

1.0 TADBIR URUS KESELAMATAN MAKLUMAT

1.1 Pentadbir Rangkaian Dan Keselamatan

1.1.1 Peranan dan tanggungjawab Pentadbir Rangkaian Dan Keselamatan adalah seperti berikut:

1.1.1.1 Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di SKM beroperasi sepanjang masa;

1.1.1.2 Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;

1.1.1.3 Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada;

1.1.1.4 Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;

1.1.1.5 Melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT (*Security Posture Assessment* (SPA)) serta penilaian risiko keselamatan maklumat;

1.1.1.6 Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian SKM secara tidak sah seperti melalui peralatan *modem* dan *dial-up*;

1.1.1.7 Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian;

1.1.1.8 Memantau penggunaan rangkaian dan melaporkan kepada Pengarah Bahagian Pengurusan Maklumat (BPM) untuk dibawa ke Ketua Pegawai Maklumat (CIO) SKM sekiranya berlaku penyalahgunaan sumber rangkaian; dan

1.1.1.9 Memastikan maklumat perhubungan perlu dikemaskini dari semasa ke semasa.

1.2 Pentadbir Pangkalan Data

1.2.1 Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut:

1.2.1.1 Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;

1.2.1.2 Memastikan pangkalan data boleh digunakan pada setiap masa;

1.2.1.3 Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;

1.2.1.4 Melaksanakan *data masking* dalam menyediakan data latihan;

1.2.1.5 Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;

1.2.1.6 Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip DKICT;

1.2.1.7 Melaksanakan proses perkemasan data (*housekeeping*) di dalam pangkalan data;

1.2.1.8 Melaksanakan proses *backup* dan *restoration* ke atas pangkalan data; dan

1.2.1.9 Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada Pengarah BPM untuk dibawa ke CIO.

1.3 Pentadbir Portal (*Web Master*)

1.3.1 Peranan dan tanggungjawab Pentadbir Portal adalah seperti berikut dan dikawal selia oleh Unit Hal Ehwal Antarabangsa dan Komunikasi Korporat (UAKK):

1.3.1.1 Menerima kandungan portal yang telah disahkan kesahihan dan terkini daripada sumber yang sah;

1.3.1.2 Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar;

1.3.1.3 Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka portal;

1.3.1.4 Mengehadkan capaian Pentadbir Portal bahagian ke *web server*;

1.3.1.5 Mengasingkan kandungan dan aplikasi dalam talian untuk capaian secara Intranet dan Internet ke portal SKM;

1.3.1.6 Memastikan hanya maklumat yang bersifat terbuka dipaparkan di portal;

1.3.1.7 Memastikan reka bentuk portal dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi;

1.3.1.8 Melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di *web server*;

1.3.1.9 Melaksanakan proses *backup* dan *restoration* ke atas kandungan dan aplikasi portal; dan

1.3.1.10 Melapor sebarang pelanggaran keselamatan portal kepada Pengarah BPM untuk dibawa ke CIO.

1.4 Pentadbir Pusat Data

1.4.1 Peranan dan tanggungjawab Pentadbir Pusat Data adalah seperti berikut:

1.4.1.1 Memastikan persekitaran fizikal dan keselamatan pusat data berada dalam keadaan baik dan selamat;

1.4.1.2 Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;

1.4.1.3 Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;

1.4.1.4 Menyediakan perancangan pemulihan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) dalam DKICT;

1.4.1.5 Melaksanakan prinsip-prinsip DKICT;

1.4.1.6 Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan;

1.4.1.6.1 Pegawai Yang Dibertanggungjawab: *Thumbprint,*

1.4.1.6.2 Pelawat/ Bahagian Lain: Buku Log Pelawat.

1.4.1.7 Melaporkan sebarang pelanggaran keselamatan Pusat Data SKM kepada Pengarah BPM untuk dibawa ke CIO; dan

1.4.1.8 Memastikan maklumat perhubungan perlu dikemaskini dari semasa ke semasa.

1.5 Pentadbir Sistem Aplikasi

1.5.1 Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut dan dikawal selia oleh Bahagian Pengurusan Maklumat (BPM) dan Pegawai Maklumat (IO) Negeri:

1.5.1.1 Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di SKM;

1.5.1.2 Membuat kajian semula serta memperbaiki sistem atau modul sedia ada di SKM;

1.5.1.3 Membuat pertimbangan dan mengusulkan cadangan pelaksanaan sistem atau modul di SKM;

1.5.1.4 Membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;

1.5.1.5 Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul;

1.5.1.6 Menyediakan dokumentasi sistem atau modul dan manual pengguna;

1.5.1.7 Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas;

1.5.1.8 Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya;

1.5.1.9 Memastikan virus *pattern*, *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam;

1.5.1.10 Mematuhi dan melaksanakan prinsip-prinsip DKICT dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi;

1.5.1.11 Mengehadkan capaian Dokumentasi Sistem Aplikasi bagi menggelakkan dari penyalahgunaannya; dan

1.5.1.12 Melaporkan kepada Pengarah BPM untuk dibawa ke CIO jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya.

1.6 Pentadbir E-mel

1.6.1 Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut:

1.6.1.1 Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan Akaun (pengguna yang bertukar, tidak lagi berkhidmat dengan SKM dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat;

1.6.1.2 Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib;

1.6.1.3 Memastikan pengguna e-mel SKM berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel SKM dan Internet SKM serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan;

1.6.1.4 Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi;

1.6.1.5 Mengesah dan memaklumkan kepada Pengarah BPM untuk dibawa ke CIO sekiranya mengalami insiden keselamatan melalui saluran rasmi; dan

1.6.1.6 Memastikan maklumat perhubungan perlu dikemaskini dari semasa ke semasa.

1.7 Pegawai Aset

1.7.1 Pegawai Aset ialah pegawai yang dilantik oleh Ketua Jabatan. Peranan dan tanggungjawab Pegawai Aset perlu merujuk kepada Tatacara Pengurusan Aset dan Stor Suruhanjaya Koperasi Malaysia. Berikut adalah antara peranan dan tanggungjawab pegawai aset bagi pengurusan aset ICT:

1.7.1.1 Memastikan pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan;

1.7.1.2 Memastikan penerimaan aset ICT Kerajaan dilaksanakan oleh pegawai yang dilantik secara bertulis oleh Ketua Jabatan/ Bahagian;

1.7.1.3 Memastikan semua aset ICT Kerajaan yang diterima, didaftarkan menggunakan Sistem Pemantauan Pengurusan Aset (SPA) dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset;

1.7.1.4 Memastikan semua aset ICT Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset;

1.7.1.5 Memastikan Daftar Aset ICT dikemas kini apabila berlaku penambahan/ penggantian/ penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;

1.7.1.6 Memastikan semua aset ICT Kerajaan diberi tanda pengenalan dengan cara melabel tanda Hak Kerajaan Malaysia dan nama SKM/ Bahagian/ Agensi berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan;

1.7.1.7 Memastikan semua aset ICT Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan;

1.7.1.8 Memastikan senarai daftar induk aset ICT Kerajaan disediakan;

1.7.1.9 Memastikan senarai aset ICT Kerajaan disediakan mengikut lokasi dan format Senarai Aset ICT Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset / Pembantu Pegawai Aset dan satu (1) salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi;

1.7.1.10 Memastikan setiap kerosakan aset ICT Kerajaan dilaporkan untuk tujuan penyelenggaraan;

1.7.1.11 Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset ICT Kerajaan;

1.7.1.12 Merancang, memantau dan memastikan pemeriksaan aset ICT Kerajaan dilaksanakan ke atas keseluruhan aset ICT Kerajaan sekurang-kurangnya sekali setahun; dan

1.7.1.13 Memastikan setiap kes kehilangan aset ICT Kerajaan dilaporkan dan diuruskan dengan teratur.

1.8 Pasukan Tindak Balas Insiden

1.8.1 Peranan dan tanggungjawab SKMCERT adalah seperti berikut:

1.8.1.1 Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;

1.8.1.2 Merekod dan menjalankan siasatan awal insiden yang diterima;

1.8.1.3 Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum;

1.8.1.4 Menghubungi dan melaporkan insiden yang berlaku kepada CIO dan pihak *National Cyber Security Agency* (NACSA) sama ada sebagai input atau untuk tindakan seterusnya;

1.8.1.5 Merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; dan

1.8.1.6 Melaporkan sebarang maklum balas dan insiden keselamatan ICT kepada CIO.

1.9 Peranan *Information Officer* (IO)

1.9.1 Peranan dan tanggungjawab IO adalah seperti berikut:

1.9.1.1 Membantu BPM merancang aktiviti pelaksanaan Sistem Maklumat Suruhanjaya Ibu Pejabat dan Cawangan Negeri;

1.9.1.2 Memastikan komputer dan peralatannya serta Sistem INFOKOP dan sistem SKM yang lain dapat beroperasi dengan baik. Memastikan pegawai membuat *clean-up* pada *server* (IO Cawangan) dan juga *clients* secara berkala bagi menjimatkan ruang storan komputer;

1.9.1.3 Menghubungi pihak berkaitan sekiranya berlaku kerosakan pada perisian dan perkakasan komputer;

1.9.1.4 Bersedia membantu pegawai/ kakitangan yang menghadapi masalah dalam penggunaan komputer terutamanya berkaitan dengan Sistem SKM;

1.9.1.5 Bertindak sebagai tenaga pengajar/ orang bertanggungjawab memberi latihan dan tunjuk ajar tentang penggunaan Sistem INFOKOP dan sistem SKM yang lain;

1.9.1.6 Bertanggungjawab menjaga (*maintain*)/ menentukan kesahihan data-data yang dimasukkan dalam Sistem INFOKOP;

1.9.1.7 Membantu membuat *repair* dan *recovery data* ketika *database down* (sekiranya perlu);

1.9.1.8 Membaiki kerosakan kecil pada komputer dan peralatannya (*troubleshooting*) sama ada dari segi perisian dan perkakasan;

1.9.1.9 Menyediakan laporan-laporan yang diperlukan oleh pihak pengurusan yang berkaitan dengan perjalanan sistem dan data-data tertentu;

1.9.1.10 Membantu menyelaras program Latihan ICT Cawangan;

1.9.1.11 Bertanggungjawab menasihati pihak pengurusan di negeri dan bahagian berhubung hala tuju pelan ICT SKM;

1.9.1.12 Bertanggungjawab menerima, mengumpul dan membantu membuat pengagihan peralatan ICT sewaan/ aset ICT kepada pegawai-pegawai yang berkaitan;

1.9.1.13 Bertanggungjawab sebagai *first level support* kepada Suruhanjaya Cawangan Negeri sekiranya berlaku sebarang masalah berkaitan ICT dan melaporkan kepada BPM melalui *Helpdesk* ICT - RFS atau emel masalah tersebut untuk tindakan selanjutnya;

1.9.1.14 Memastikan talian MyGov*Net berfungsi dengan baik dan menghubungi pihak GiTN sekiranya berlaku gangguan atau kerosakan. Melaporkan kepada BPM sekiranya melibatkan keperluan/ penambahbaikan polisi baharu (akses media sosial, *upgrade bandwidth* dan lain-lain berkaitan);

1.9.1.15 Melaporkan kepada BPM sekiranya terdapat kerja pengubahsuaian pejabat/ pembukaan pejabat baharu dan penutupan pejabat (terutama yang melibatkan talian MyGov*Net) mengikut tempoh yang telah ditetapkan oleh BPM;

1.9.1.16 Membuat permohonan projek kepada BPM bagi sebarang pembelian/ sewaan aset ICT/ program atau projek melibatkan ICT untuk kelulusan Jawatankuasa Pemandu ICT (JPICT) SKM;

1.9.1.17 Bertanggungjawab mengumpul semua aset ICT yang terlibat untuk pelupusan;

1.9.1.18 Bertanggungjawab memastikan semua pegawai/ kakitangan menggunakan lesen perisian yang sah dimiliki oleh SKM; dan

1.9.1.19 Membantu pegawai penerima aset di cawangan negeri membuat semakan peralatan ICT sebelum disahkan dan diterima oleh pegawai penerima aset.

1.10 Peranan *Data Officer* (DO)

1.10.1 Peranan dan tanggungjawab DO adalah seperti berikut:

1.10.1.1 Membantu dalam menyelaras data perangkaan SKM Negeri masing-masing; dan

1.10.1.2 Penyelarasan Profil 100 Koperasi Terbaik peringkat Negeri.

PENGURUSAN ASET

SURUHANJAYA KOPERASI MALAYSIA

2.0 PENGURUSAN ASET

2.1 Aset Fizikal

Bagi pengurusan aset fizikal, rujuk Tatacara Pengurusan Aset dan Stor serta Garis Panduan Dalaman Pengurusan Penggunaan Peralatan 1.0.

2.1.1 Peminjaman dan Pemulangan Aset ICT

2.1.1.1 Peminjaman

2.1.1.1.1 Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan bagi membawa keluar peralatan bagi tujuan yang dibenarkan;

2.1.1.1.2 Melindungi dan mengawal peralatan sepanjang masa;

2.1.1.1.3 Merekodkan aktiviti peminjaman dan pemulangan peralatan; dan

2.1.1.1.4 Menyemak peralatan ketika peminjaman dan pemulangan dilakukan.

2.1.1.2 Pemulangan

Memastikan semua aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan bagi pegawai yang:

2.1.1.2.1 Bertukar keluar;

2.1.1.2.2 Bersara;

2.1.1.2.3 Ditamatkan perkhidmatan;

2.1.1.2.4 Berhenti;

2.1.1.2.5 Diarahkan oleh Ketua Jabatan untuk membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan; dan

2.1.1.2.6 Membatalkan atau menarik balik semua kebenaran capaian ke atas aset ICT mengikut peraturan yang ditetapkan.

2.1.2 Pelupusan Aset ICT

2.1.2.1 Aset ICT yang hendak dilupuskan perlu mematuhi tatacara pelupusan semasa. Langkah-langkah berikut perlu diambil dalam memastikan peralatan ICT SKM dilupuskan dengan teratur iaitu:

2.1.2.1.1 Pegawai Maklumat Negeri/ Pegawai Aset/ Pegawai Teknikal Bahagian Pengurusan Maklumat akan mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

2.1.2.1.2 Pelantikan sebagai Pegawai Pemeriksa Perakuan Pelupusan (PEP) Aset ICT dan Peralatan Komputer SKM perlu dibuat terlebih dahulu;

2.1.2.1.3 Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan;

2.1.2.1.4 Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;

2.1.2.1.5 Pelupusan peralatan ICT boleh dilakukan secara berpusat atau tidak berpusat mengikut tatacara pelupusan semasa yang berkuat kuasa;

2.1.2.1.6 Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;

2.1.2.1.7 Maklumat lanjut berhubung pelupusan boleh dirujuk kepada pekeliling perbendaharaan semasa yang berkuatkuasa; dan

2.1.2.1.8 Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan Tatacara Jabatan Arkib Negara.

2.2 Aset Bukan Fizikal

2.2.1 Pengelasan dan Pengendalian Data Terbuka

Data Terbuka ialah data yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Jabatan akan menyediakan set data terbuka berdasarkan bidang atau sektor atau kluster. Kategori set data ini tidak terhad dan boleh berubah mengikut fungsi teras dan keperluan semasa Jabatan.

Data terbuka yang telah diperakukan oleh Jabatan akan dikemukakan ke Jabatan Perdana Menteri (JPM) untuk kelulusan dan seterusnya diterbitkan ke Portal Data Terbuka Sektor Awam (DTSA) di bawah pengurusan MAMPU.

2.2.2 Pengelasan Maklumat

2.2.2.1 Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada SKM.

2.2.2.2 Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan dan dilabel sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

2.2.2.2.1 Rahsia Besar;

2.2.2.2.2 Rahsia;

2.2.2.2.3 Sulit; atau

2.2.2.2.4 Terhad.

KAWALAN CAPAIAN INTERNET

SURUHANJAYA KOPERASI MALAYSIA

3.0 KAWALAN CAPAIAN INTERNET

3.1 Pengurusan Kata Laluan

3.1.1 Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh SKM seperti berikut:

3.1.1.1 Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

3.1.1.2 Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan antara huruf dan nombor (*alphanumeric*) dan aksara khas;

3.1.1.3 Kekerapan penukaran dan penggunaan kata laluan adalah mengikut ketetapan polisi pengurusan kata laluan yang berkuatkuasa;

3.1.1.4 Kata laluan sistem pengoperasian (OS) atau *Directory Service* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama;

3.1.1.5 Kata laluan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun;

3.1.1.6 Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

3.1.1.7 Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula;

3.1.1.8 Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

3.1.1.9 Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula;

3.1.1.10 Kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan; dan

3.1.1.11 Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.

3.2 Capaian Rangkaian

3.2.1 Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

3.2.1.1 Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian SKM dan rangkaian awam;

3.2.1.2 Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dengan peralatan yang menepati kesesuaian penggunaannya;

3.2.1.3 Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

3.2.1.4 Capaian pengguna jarak jauh (*remote user*) secara *virtual private network* (VPN) perlulah dikawal dan dipantau, rujuk **Lampiran 1** bagi Borang Permohonan VPN;

3.2.1.4.1 Pengguna Berkala:

3.2.1.4.1.1 Pegawai SKM: Permohonan berdasarkan keperluan penggunaan semasa melalui e-mel bagi tujuan akses ke sistem.

3.2.1.4.1.2 Pihak Pembekal: Permohonan berdasarkan keperluan penggunaan semasa melalui e-mel bagi tujuan *patching updates* dan *troubleshooting*.

3.2.1.4.2 Pengguna Berterusan: Permohonan berdasarkan keperluan untuk membuat *monitoring system* secara berterusan.

3.2.1.5 Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal; dan

3.2.1.6 Semua rangkaian yang dikongsi (*shared networks*), terutama yang keluar daripada rangkaian SKM, polisi perlu diwujudkan untuk mengawal capaian oleh pengguna.

3.3 Capaian Internet

3.3.1 Penggunaan Internet di SKM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian dan Keselamatan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian SKM;

3.3.2 Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. CIO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

3.3.3 Polisi *Content Filtering* mestilah digunakan dan dipantau bagi mengawal akses Internet. Pengguna boleh memohon pengecualian mengikut fungsi kerja untuk pertimbangan;

3.3.4 Penggunaan proksi yang telah ditetapkan oleh SKM bagi mengawal akses Internet mengikut fungsi kerja dan mematuhi pekeliling semasa yang dikeluarkan; dan

3.3.5 Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan.

3.4 Hak Capaian (*Access Privilege*)

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat, atas prinsip perlu mengetahui (*need to know basis*). Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.

3.5 Capaian Aplikasi dan Maklumat

3.5.1 Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

3.5.2 Capaian sistem dan aplikasi di SKM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut perlu dipatuhi:

3.5.2.1 Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;

3.5.2.2 Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (*log*) bagi mengesan aktiviti-aktiviti yang tidak diingini;

3.5.2.3 Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;

3.5.2.4 Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah;

3.5.2.5 Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja;

3.5.2.6 Maklumat tarikh *login* terakhir hendaklah direkodkan; dan

3.5.2.7 *Session timeout* hendaklah dilaksanakan:

3.5.2.7.1 Sistem Kritikal = 200 saat
3.5.2.7.2 Lain-Lain = 600 saat
3.5.2.7.3 Sistem SAGA = 1200 saat

3.5.3 Permohonan Akses ID Sistem mestilah melalui pemilik sistem dan untuk pengesahan maklumat (tambahan).

3.6 Capaian Jarak Jauh

3.6.1 Capaian jarak jauh yang dimaksudkan merangkumi:

3.6.1.1 Capaian daripada sistem rangkaian dalaman; dan

3.6.1.2 Capaian daripada sistem rangkaian luaran bagi lokasi pejabat untuk tujuan *telecommuting.*

3.6.2 Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*);

3.6.3 Lokasi bagi akses ke sistem ICT SKM hendaklah dipastikan selamat; dan

3.6.4 Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan Pengguna yang diberi hak adalah dipertanggungjawab penuh ke atas penggunaan kemudahan ini.

3.7 Permohonan MyGov*Net

Sekiranya terdapat kerja pengubahsuaian pejabat/pembukaan pejabat baharu dan penutupan pejabat, permohonan MyGov*Net perlu dihantar kepada BPM dalam tempoh tiga (3) bulan sebelum tarikh bermula.

3.8 Penggunaan Sidang Video

Penggunaan sidang video adalah meliputi perkara-perkara yang berkaitan dengan pengurusan sidang video, aktiviti mesyuarat, *live streaming*, perkakasan sidang video dan perkara yang berkaitan hanya dibenarkan untuk kegunaan yang melibatkan urusan rasmi dan kerja sahaja.

KESELAMATAN PERALATAN ICT

SURUHANJAYA KOPERASI MALAYSIA

4.0 KESELAMATAN PERALATAN ICT

4.1 Peralatan ICT

4.1.1 Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

4.1.1.1 Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

4.1.1.2 Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

4.1.1.3 Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem Aplikasi;

4.1.1.4 Pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh Jabatan seperti komputer peribadi, *notebook*, *server* dan lain-lain yang berada di bawah tanggungjawab mereka sentiasa aktif (*activated*) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan;

4.1.1.5 Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salahguna;

4.1.1.6 Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang

bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset;

4.1.1.7 Sekiranya peralatan ICT tidak digunakan, peralatan tersebut hendaklah disimpan di dalam almari atau kabinet atau peti besi atau stor atau bilik khas yang berkunci untuk penyimpanan peralatan ICT;

4.1.1.8 Peralatan ICT yang kritikal perlu disokong oleh UPS;

4.1.1.9 UPS yang berkuasa tinggi perlu diletakkan di bilik yang berasingan bersuhu rendah yang dilengkapi dengan pengudaraan yang sesuai;

4.1.1.10 Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam bilik atau rak berkunci;

4.1.1.11 Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

4.1.1.12 Peralatan ICT yang hendak dibawa keluar dari premis SKM, perlulah mendapat kelulusan Pengarah BPM/Pegawai Aset/IO atau Penyelaras ICT Bahagian bagi tujuan pemantauan; dan

4.1.1.13 Aset ICT yang hilang hendaklah dilaporkan mengikut pekeliling perbendaharaan sedia ada.

4.2 Perisian dan Aplikasi

4.2.1 Sebarang perisian dan aplikasi yang digunakan hendaklah mematuhi langkah–langkah berikut:

4.2.1.1 Hanya perisian yang rasmi sahaja dibenarkan bagi kegunaan jabatan;

4.2.1.2 Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-ROM, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak;

4.2.1.3 Kod sumber (*source code*) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; dan

4.2.1.4 Sistem aplikasi, perisian dan kod sumber tidak dibenarkan dikongsi, diagih, dibawa keluar atau didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT.

4.3 Penyelenggaraan peralatan ICT

4.3.1 Peralatan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut:

4.3.1.1 Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;

4.3.1.2 Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;

4.3.1.3 Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan

4.3.1.4 Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

4.4 Kabel Rangkaian ICT

4.4.1 Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat;

4.4.2 Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; dan

4.4.3 Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wiretapping*.

KESELAMATAN OPERASI

SURUHANJAYA KOPERASI MALAYSIA

5.0 KESELAMATAN OPERASI

5.1 Pengasingan Tugas dan Tanggungjawab

5.1.1 Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

5.1.1.1 Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

5.1.1.2 Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah dilakukan oleh pegawai yang berlainan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan

5.1.1.3 Perkakasan dan rangkaian yang digunakan bagi tugas membangun, mengemaskini, dan menguji aplikasi hendaklah diasingkan dari perkakasan dan rangkaian yang digunakan di dalam persekitaran pembangunan dan pengujian, peringkat *staging* dan produksi.

5.2 Perancangan dan Penerimaan Sistem

5.2.1 Perancangan

5.2.1.1 Perkara yang perlu dipatuhi adalah seperti berikut:

5.2.1.1.1 Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi

memastikan keperluanmnya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan

5.2.1.1.2 Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

5.2.2 Penerimaan Sistem

Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

5.3 Perlindungan dari Perisian Berbahaya (Virus)

5.3.1 Perkara yang perlu dipatuhi adalah seperti berikut:

5.3.1.1 Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya (seperti *anti-virus, anti-spyware, anti-spam, content filtering, web reputation dan Intrusion Prevention System* (IPS)) dan mengikut prosedur penggunaan yang betul dan selamat;

5.3.1.2 Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

5.3.1.3 Mengimbas semua data, perisian atau sistem dengan perisian keselamatan yang bersesuaian sebelum menggunakannya;

5.3.1.4 Mengemas kini perisian keselamatan dari semasa ke semasa;

5.3.1.5 Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

5.3.1.6 Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

5.3.1.7 Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

5.3.1.8 Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian/aplikasi yang dibangunkan; dan

5.3.1.9 Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

5.4 Pengauditan dan Forensik ICT

5.4.1 SKMCERT mestilah bertanggungjawab merekod dan menganalisis:

5.4.1.1 Sebarang percubaan pencerobohan kepada sistem ICT SKM;

5.4.1.2 Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*) *spam*,

pemalsuan (*forgery*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);

5.4.1.3 Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak;

5.4.1.4 Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan;

5.4.1.5 Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan;

5.4.1.6 Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian;

5.4.1.7 Aktiviti penyalahgunaan akaun e-mel; dan

5.4.1.8 Aktiviti penukaran IP *address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian dan Keselamatan.

5.4.2 Langkah-langkah yang perlu diambil adalah seperti berikut:

5.4.2.1 SKMCERT akan menentukan prosedur pengumpulan bahan bukti (*hard disk* atau media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan;

5.4.2.2 Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan

5.4.2.3 Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, format laporan khas perlu disediakan.

Semua proses dan hasil siasatan adalah **SULIT**.

5.5 Sistem *Log* (*log* sistem untuk tujuan pemantauan, analisa keselamatan ICT)

5.5.1 Fail *log* hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail *log* bagi *server* dan aplikasi yang perlu diaktifkan adalah seperti berikut:

5.5.1.1 Fail *log* sistem pengoperasian;

5.5.1.2 Fail *log* servis (contoh: *web, e-mel*);

5.5.1.3 Fail *log* aplikasi (*audit trail*); dan

5.5.1.4 Fail *log* rangkaian (contoh: *switch*, *firewall*, IPS).

5.5.2 Pentadbir Sistem Aplikasi hendaklah melaksanakan perkara-perkara berikut:

5.5.2.1 Mewujudkan sistem *log* bagi merekodkan semua aktiviti harian pengguna;

5.5.2.2 Menyemak sistem *log* secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

5.5.2.3 Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada CIO.

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

SURUHANJAYA KOPERASI MALAYSIA

6.0 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

6.1 Pengesahan Data *Input*

Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.

6.2 Pengesahan Data *Output*

Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

6.3 Peraturan Keselamatan Dalam Pembangunan Sistem Aplikasi

Tatacara pembangunan perisian dan sistem aplikasi yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.

6.4 Kawalan Terhadap Perubahan Kepada Perisian

Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.

6.5 Persekitaran Pembangunan Sistem Aplikasi Yang Selamat

Persekitaran pembangunan sistem aplikasi yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.

6.6 Pembangunan Sistem Secara Penyumberan Luar (*Outsource*)

6.6.1 Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut:

6.6.1.1 Setiap projek perlu dipantau oleh CIO;

6.6.1.2 Kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik SKM;

6.6.1.3 Kod sumber yang diserahkan kepada SKM mesti bebas daripada sebarang ralat dan kerentanan;

6.6.1.4 Mengutamakan kepakaran teknologi tempatan;

6.6.1.5 Pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran SKM;

6.6.1.6 Penggunaan *data masking* semasa pengujian;

6.6.1.7 Data ujian hendaklah dilupuskan secara kekal (*secured delete*) selepas projek disiapkan/tamat kontrak; dan

6.6.1.8 Aktiviti sandaran hendaklah berjaya dilakukan sebelum projek tamat.

6.7 Ujian Keselamatan Sistem

Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.

6.8 Pembocoran Maklumat

Sebarang peluang untuk membocorkan maklumat melalui apa cara sekalipun mestilah dihalang.

RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

SURUHANJAYA KOPERASI MALAYSIA

7.0 RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

7.1 Mekanisme Pelaporan Insiden Keselamatan ICT

7.1.1 Pelaporan

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan segera kepada SKMCERT untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian. Semua maklumat adalah **SULIT**, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Antara insiden keselamatan ICT yang perlu dilaporkan adalah:

7.1.1.1 Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

7.1.1.2 Sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian;

7.1.1.3 Kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian;

7.1.1.4 Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan

7.1.1.5 Berlaku percubaan menceroboh, penyelewengan dan insiden- insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT.

7.1.2 Pelaporan NACSA

7.1.2.1 CIO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu;

7.1.2.2 Pasukan SKMCERT dengan persetujuan CIO akan menghubungi NACSA untuk melapor atau mendapatkan bantuan apabila wujud potensi insiden atau berlaku sebarang insiden keselamatan ICT;

7.1.2.3 Tindakan Dalam Keadaan Berisiko Tinggi

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak;

7.1.2.4 CIO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu; dan

7.1.2.5 Insiden Keselamatan Sistem - Pentadbir Sistem Aplikasi yang terlibat mesti melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada SKMCERT.

7.2 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT

7.2.1 Pasukan SKMCERT perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT.

7.2.2 Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada pihak NACSA.

7.2.3 Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang. SKMCERT yang diketuai oleh CIO akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *on-site*.

7.2.4 Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA.

7.2.5 Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihak NACSA dan khidmat nasihat akan disalurkan. SKMCERT seterusnya akan menyediakan laporan dan CIO mengesahkan sekiranya PKP perlu diaktifkan atau sebaliknya.

7.2.6 Pengesahan akan dihantar kepada CIO bagi mengaktifkan PKP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.

7.2.7 Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan, mengikut prosedur dengan mengambil kira kawalan-kawalan berikut:

7.2.7.1 Mengenal pasti semua jenis insiden keselamatan ICT;

7.2.7.2 Mematuhi Pelan Pemulihan Bencana (DRP) seperti yang telah digariskan dalam Pengurusan Kesinambungan Perkhidmatan (PKP);

7.2.7.3 Sistem SAGA SKM-FS rujuk Pelan Pemulihan Bencana versi 4.1;

7.2.7.4 Sistem lain hanya membuat *backup* dan *restore* secara manual dan akan dilaksanakan DRP apabila sistem utama SKM yang baharu dibangunkan;

7.2.7.5 Menyimpan jejak audit dan memelihara bahan bukti dan rekod;

7.2.7.6 Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan

7.2.7.7 Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

7.3 *Backup Data*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan (senarai semak) hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah:

7.3.1 Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu;

7.3.2 Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi;

7.3.3 Menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan

7.3.4 *Backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.

7.4 Peraturan Keselamatan Dalam Pembangunan Sistem

Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.

7.5 Kawalan Terhadap Perubahan Kepada Perisian

Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.

7.6 Persekitaran Pembangunan Sistem Yang Selamat

Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.

7.7 Ujian Keselamatan Sistem

Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.

7.8 Aduan Kerosakan ICT (*Request For Service* (RFS))

Sebarang kerosakan ICT perlulah menggunakan sistem RFS. Tempoh masa bagi penyelesaian masalah:

7.8.1 Masa Tindak Balas (*Response Time*): Enam (6) jam selepas menerima aduan atau mengikut *service level agreement* (SLA) yang telah ditetapkan di dalam kontrak perjanjian.

7.8.2 Tempoh Penyelesaian Masalah (*Resolution Time*): Dalam tempoh satu (1) hari bekerja berikutnya setelah menerima aduan atau mengikut *service level agreement* (SLA) yang telah ditetapkan di dalam kontrak perjanjian.

7.8.3 Kaedah Khidmat Sokongan / Tindakan: Atas talian (telefon, e-mel, *whatsapp*, *remote*, *web helpdesk*).

KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

SURUHANJAYA KOPERASI MALAYSIA

8.0 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

8.1 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

8.1.1 ***Backup Data***

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* seperti yang dibutirkan (senarai semak) hendaklah dilakukan setiap kali konfigurasi berubah. *Backup* hendaklah direkodkan dan disimpan di *off site*, di antaranya adalah:

8.1.1.1 Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu;

8.1.1.2 Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi;

8.1.1.3 Menguji sistem *backup* sedia ada dan bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan

8.1.1.4 *Backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.

8.1.2 **Peraturan Keselamatan Dalam Pembangunan Sistem**

Tatacara pembangunan perisian dan sistem yang mengambil kira aspek keselamatan maklumat hendaklah diwujudkan dan dilaksanakan di dalam organisasi.

8.1.3 **Kawalan Terhadap Perubahan Kepada Perisian**

Sebarang perubahan terhadap perisian adalah tidak digalakkan, kecuali kepada perubahan yang perlu sahaja dan perubahan tersebut perlu dihadkan.

8.1.4 **Persekitaran Pembangunan Sistem Yang Selamat**

Persekitaran pembangunan sistem yang selamat perlu diwujudkan sepanjang kitar hayat pembangunan sistem.

8.1.5 **Ujian Keselamatan Sistem**

Aktiviti pengujian keselamatan sistem hendaklah dilaksanakan atas sistem baharu, tambah baik, naik taraf dan versi baharu berdasarkan kriteria yang telah ditetapkan.

8.1.6 **Aduan Kerosakan ICT (*Request For Service* (RFS))**

Sebarang kerosakan ICT perlulah menggunakan sistem RFS. Tempoh masa bagi penyelesaian masalah:

8.1.6.1 Masa Tindak Balas (*Response Time*): Enam (6) jam selepas menerima aduan atau mengikut *service level agreement* (SLA) yang telah ditetapkan di dalam kontrak perjanjian.

8.1.6.2 Tempoh Penyelesaian Masalah (*Resolution Time*): Dalam tempoh satu (1) hari bekerja berikutnya setelah menerima aduan atau mengikut *service level agreement* (SLA) yang telah ditetapkan di dalam kontrak perjanjian.

8.1.6.3 Kaedah Khidmat Sokongan/ Tindakan: Atas talian (telefon, e-mel, *whatsapp*, *remote*, w*eb helpdesk*).

PEMATUHAN

SURUHANJAYA KOPERASI MALAYSIA

9.0 PEMATUHAN

9.1 PEMATUHAN

9.1.1 Peraturan dan Penilaian Teknikal Keselamatan ICT

9.1.1.1 CIO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.

9.1.1.2 Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan.

9.1.1.3 Sebarang penilaian pematuhan teknikal mestilah dijalankan oleh individu yang kompeten dan dibenarkan.

9.1.1.4 Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.

9.1.1.5 Keperluan audit dan sebarang aktiviti pemerikasaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.

9.1.1.6 Capaian ke atas peralatan audit sistem maklumat perlu dikawal dan diselia bagi mengelakkan berlaku penyalahgunaan.

GLOSARI

SURUHANJAYA KOPERASI MALAYSIA

GLOSARI

PERKATAAN	MAKSUD
LAN	*Local Area Network*
WAN	*Wide Area Network*
UPS	*Uninterruptible Power Supply*
CIO	*Chief Information Officer*
PKP	Pengurusan Kesinambungan Perkhidmatan
DRP	Pelan Pemulihan Bencana
NACSA	*National Cyber Security Agency*
DTSA	Portal Data Terbuka Sektor Awam
IPS	*Intrusion Prevention System*
SPA	Sistem Pemantauan Pengurusan Aset
OS	*Operating System*
SLA	*Service Level Agreement*
VPN	*Virtual Private Network*
IO	*Information Officer* *(*Pegawai Maklumat SKM yang dilantik oleh Pengarah Ibu Pejabat dan Cawangan Negeri*)*
DO	*Data Officer* *(*Pegawai Data SKM yang dlantik oleh Pengarah Negeri*)*
SKMCERT	*Computer Emergency Response Team* Agensi. Pasukan yang dtubuhkan untuk membantu Suruhanjaya mengurus pengendalian insiden keselamatan ICT di SKM.
CERT	Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan

PENTADBIR SISTEM APLIKASI	Pegawai yang bertanggungjawab untuk menyelanggara, mengkonfigurasi dan mengendalikan sistem komputer, terutamanya komputer berbilang pengguna seperti pelayan.
PENTADBIR RANGKAIAN DAN KESELAMATAN	Pegawai yang ditugaskan untuk menjaga, memantau dan memastikan kelancaran operasi dan infrastruktur rangkaian.
PENTADBIR PORTAL	Pentadbir Portal adalah merupakan pegawai yang dilantik oleh Jabatan untuk menguruskan Portal SKM.
PEMILIK SISTEM	Pemilik *business process* yang menggunakan sistem sebagai operasi bahagian dan jabatan.
PENTADBIR EMEL	Pentadbir sistem e-mel merupakan Pegawai Bahagian Pengurusan Maklumat yang menguruskan operasi sistem e-mel SKM.
PEGAWAI ASET	Mengetuai Bahagian/Seksyen/Unit Pengurusan Aset (UPA) bagi memastikan Pengurusan Aset Alih Kerajaan dijalankan selaras dengan peraturan yang ditetapkan dalam Tatacara Pengurusan Aset SKM.

LAMPIRAN

SURUHANJAYA KOPERASI MALAYSIA

LAMPIRAN 1

BORANG PERMOHONAN VPN

SURUHANJAYA KOPERASI MALAYSIA

LAMPIRAN 1: BORANG PERMOHONAN VPN

BORANG PERMOHONAN
***VIRTUAL PRIVATE NETWORK* (VPN)**
SURUHANJAYA KOPERASI MALAYSIA

VPN Kakitangan SKM	☐
VPN Pembekal	☐

Kepada: Pengarah Bahagian Pengurusan Maklumat

BIL	PERKARA	MAKLUMAT
1.	Nama Pemohon* (Huruf Besar)	
2.	Jawatan*	
3.	Nombor Kad Pengenalan / *Passport**	
4.	Warganegara*	
5.	Alamat E-mel Rasmi*	
6.	No. Telefon*	
7.	Nama Organisasi / Pembekal*	
8.	Alamat Organisasi / Pembekal*	
9.	Nyatakan permohonan atau penamatan dan kegunaan akses VPN	**PERLU DI TANDA:** ☐ **PERMOHONAN AKAUN VPN** ☐ **PENAMATAN AKAUN VPN**
	TEMPOH KEGUNAAN VPN **TARIKH MULA :** **TARIKH TAMAT :**	**TUJUAN PERMOHONAN AKAUN VPN** .....

Saya akan mematuhi segala peraturan yang termaktub dalam Akta Rahsia Rasmi 1972, Akta Jenayah Komputer 1997, Akta Komunikasi dan Multimedia 1998 serta semua pekeliling dan peruntukan berkaitan dengan perlindungan maklumat dan rahsia Kerajaan Malaysia. Saya juga akan memaklumkan kepada pihak Bahagian Pengurusan Maklumat, SKM mengenai penamatan perkhidmatan saya sebagai kakitangan organisasi yang tersebut di atas atau apabila kontrak organisasi dengan SKM tamat dengan mengisi dan menghantar Borang Permohonan Penamatan Virtual Private Network (VPN) SKM. Saya juga bersetuju:

Tandatangan & Nama Penuh

.....

Tarikh :

Pengesahan & Tandatangan Pegawai BPM

.....

Tarikh :

LAMPIRAN 2

GARIS PANDUAN PENGURUSAN PENGGUNAAN PERALATAN ICT 1.0

SURUHANJAYA KOPERASI MALAYSIA

LAMPIRAN 2: GARIS PANDUAN PENGURUSAN PENGGUNAAN PERALATAN ICT 1.0

SURUHANJAYA KOPERASI Malaysia

GARIS PANDUAN DALAMAN
PENGURUSAN PENGGUNAAN PERALATAN ICT
SURUHANJAYA KOPERASI MALAYSIA

1. PENGENALAN

1.1 Garis panduan ini bertujuan untuk menjelaskan dasar serta panduan kepada warga Suruhanjaya Koperasi Malaysia (Suruhanjaya) berkaitan pengurusan penggunaan peralatan ICT di Suruhanjaya.

Garis Panduan ini meliputi perkara berikut:

(a) Kelayakan agihan peralatan ICT;
(b) Pengagihan peralatan ICT;
(c) Tatacara penggunaan, penjagaan dan penyimpanan; dan
(d) Prosedur kerosakan atau kehilangan peralatan ICT.

1.2 Dalam Garis panduan ini , melainkan jika konteks mengkehendaki makna yang lain-

(a) 'Peralatan ICT' terdiri daripada perkakasan dan ditakrifkan di bawah Katalog Peralatan dan Kelengkapan ICT dalam Pusat Rujukan Maklumat Aset Awam Kementerian Kewangan Malaysia http://knowledgebase.treasury.gov.my/knowledgebase/

(b) 'Komputer tablet' merujuk kepada komputer tablet yang disewa daripada pembekal tertakluk kepada syarat yang dipersetujui bersama.

2. LATAR BELAKANG

2.1 Bahagian Pengurusan Maklumat (BPM) bertanggungjawab untuk memastikan sumber ICT disedia dan digunakan secara optimum bagi meningkatkan kecekapan perkhidmatan pentadbiran dan sokongan Suruhanjaya.

2.2 Bagi peralatan ICT, BPM secara amnya akan menyelaras dan menyeragamkan pengagihan peralatan tersebut untuk mengelakkan pembaziran sumber dan menjimatkan kos serta memudahkan kerja penyelenggaraan. BPM juga bertanggungjawab untuk menguruskan pengagihan peralatan ICT bagi Ibu Pejabat Suruhanjaya manakala Pengarah Negeri dipertanggungjawabkan untuk menguruskan pengagihan peralatan ICT bagi Negeri/ Wilayah.

3. KEPERLUAN PERALATAN ICT

3.1 Kajian Awal Keperluan Peralatan ICT

Kajian awal keperluan peralatan ICT dilaksana dan diedarkan pada setiap negeri dan wilayah bagi mendapatkan data keperluan peralatan ICT.

3.2 Kelayakan Agihan

Kelayakan pengagihan peralatan ICT dilaksanakan mengikut **Garis Panduan Mengenai Pengagihan Peralatan ICT di Suruhanjaya Koperasi Malaysia** bertarikh 16 Oktober 2019.

4. PENGAGIHAN PERALATAN ICT

4.1 Jenis Peralatan ICT

(a) Peralatan ICT bagi kegunaan warga Suruhanjaya termasuk berikut:

(i) Komputer Peribadi;
(ii) Komputer Riba;
(iii) LCD Projektor;
(iv) Pengimbas;
(v) Pencetak (berwarna atau tidak berwarna); dan
(vi) Komputer Tablet.

(b) Komputer tablet hanya boleh dibekalkan sebanyak satu (1) unit sahaja kepada Pengerusi Eksekutif, Timbalan Pengerusi Eksekutif,

Naib Pengerusi Eksekutif, Pengarah Bahagian dan Negeri yang layak. Polisi pengagihan komputer tablet adalah berdasarkan kepada kelayakan jawatan di Suruhanjaya.

4.2 Penyelarasan pengagihan peralatan ICT akan dilaksanakan oleh BPM bersama pembekal yang dilantik. Manakala bagi pengagihan komputer tablet, BP akan menyelaraskan pengagihannya bersama pembekal yang telah dilantik.

4.3 Proses Pengagihan Peralatan ICT di Suruhanjaya adalah seperti berikut:

(a) Di peringkat Ibu Pejabat

(i) Pembekal yang dilantik akan membuat penghantaran dan pemasangan peralatan ICT di Ibu Pejabat.

(ii) Pegawai BPM akan menyemak dan mengesahkan penerimaan peralatan ICT tersebut berdasarkan spesifikasi yang diberikan sebelum dibuat pengagihan.

(iii) Pegawai BPM akan membuat pengujian peralatan ICT bersama pihak pembekal menerusi **borang *User Acceptance Test* (UAT)**.

(iv) Pengagihan dan penggunaan peralatan ICT sewaan bagi Ibu Pejabat akan direkodkan oleh BPM (atau BP, dalam hal komputer tablet) melalui Borang Aku Janji **Lampiran A** dan Borang Pergerakan Peralatan ICT Sewaan seperti di **Lampiran B**;

(v) Bagi pengagihan peralatan ICT kategori aset, peralatan tersebut perlu didaftarkan dan direkodkan menggunakan borang KEW.PA-3 dan KEW.PA-4.

(b) Di peringkat Suruhanjaya Negeri

(i) Pihak BPM akan menyalurkan maklumat spesifikasi peralatan ICT termasuk jumlah serta jenis peralatan yang terlibat kepada *Information Officer* (IO) Negeri (SKM Negeri/ Wilayah) sebelum peralatan ICT diterima.

(ii) Pembekal yang dilantik akan membuat penghantaran dan pemasangan peralatan ICT di lokasi mengikut tempoh yang telah diselaraskan oleh BPM.

(iii) IO Negeri akan menyemak dan mengesahkan penerimaan peralatan ICT tersebut berdasarkan spesifikasi yang diberikan sebelum pengagihan dibuat.

(iv) IO Negeri akan membuat pengujian peralatan ICT bersama pihak pembekal menerusi **borang *User Acceptance Test* (UAT)**.

(v) Pengaktifan penggunaan komputer riba dan komputer peribadi akan dimaklumkan oleh BPM melalui emel kepada penerima dan pemakluman kepada IO Negeri.

(vi) Pengagihan dan penggunaan peralatan ICT sewaan bagi SKM Negeri dan Wilayah akan direkodkan oleh BPM melalui Borang Aku Janji **Lampiran C**;

5. PENGGUNAAN PERALATAN ICT

5.1 Semua peralatan ICT **tidak dibenarkan** dibawa keluar dari pejabat kecuali dengan kebenaran secara bertulis Ketua Jabatan.

5.2 Peraturan penggunaan peralatan ICT hendaklah mematuhi tatacara berikut:

(a) Digunakan oleh warga Suruhanjaya yang masih berkhidmat bagi tujuan tugas rasmi sahaja;

(b) Warga Suruhanjaya yang telah menerima komputer riba perlu mendapatkan kebenaran daripada Ketua Jabatan sekiranya terdapat keperluan untuk dipindah milik;

(c) Warga Suruhanjaya bertanggungjawab sepenuhnya ke atas penggunaan peralatan ICT yang dibekalkan dan perlu menjaga keselamatan peralatan tersebut dan maklumat Kerajaan yang tersimpan di dalamnya;

(d) Warga Suruhanjaya akan dipertanggungjawabkan ke atas sebarang penyalahgunaan peralatan ICT sekiranya peralatan tersebut digunakan oleh pihak lain;

(e) Peralatan ICT gunasama yang dibenarkan dibawa keluar dari Suruhanjaya untuk tujuan rasmi perlu mendapat kebenaran BPM (bagi Ibu Pejabat) dan kebenaran terlebih dahulu Ketua Jabatan (bagi di Suruhanjaya Negeri) berdasarkan kepada kriteria berikut:

(i) Semua warga Suruhanjaya adalah bertanggungjawab sepenuhnya ke atas peralatan ICT yang dibawa keluar dari Suruhanjaya;

(ii) Semua peralatan ICT dan aksesori hendaklah digunakan dengan baik dan sentiasa berada dalam keadaan lengkap, bersih dan sempurna sepertimana semasa ianya diterima;

(iii) Bagi memelihara keselamatan maklumat terperingkat, warga Suruhanjaya yang menerima/menggunakan peralatan ICT hendaklah mematuhi Arahan Keselamatan Kerajaan dan Polisi/ Arahan Keselamatan Perkongsian Maklumat SKM.

6. PENJAGAAN DAN PENYIMPANAN PERALATAN ICT (TERMASUK KOMPUTER TABLET)

Secara umumnya, penggunaan, penjagaan dan penyimpanan peralatan ICT adalah termaktub dalam Tatacara Pengurusan Aset Alih Bagi Suruhanjaya Koperasi Malaysia Pekeliling yang dikuatkuasa 3 Februari 2022 dan sebarang pindaan yang dibuat atasnya.

6.1 Penjagaan dan Penyimpanan Semasa di Pejabat

(a) Peralatan ICT bagi warga Suruhanjaya yang dipertanggungjawabkan:

(i) Peralatan ICT hendaklah sentiasa berada di bawah kawalan dan pengawasan warga Suruhanjaya yang dipertanggungjawabkan.

(ii) Komputer riba yang digunakan hendaklah sentiasa dikunci menggunakan *safety lock* yang telah dibekalkan oleh BPM (bagi Ibu Pejabat) dan IO Negeri (bagi Negeri/ Wilayah) sewaktu pengagihan/penerimaan peralatan tersebut.

(iii) Komputer riba dan komputer tablet yang tidak digunakan dalam tempoh masa yang lama tidak digalakkan diletakkan di atas meja sebaliknya hendaklah disimpan di dalam almari/ kabinet besi yang berkunci.

(iv) Semua peralatan ICT yang dipertanggungjawabkan (seperti pencetak, pengimbas) perlu disimpan atau ditempatkan di lokasi yang selamat.

(b) Peralatan ICT gunasama (*pool* di BPM)

(i) Permohonan Pinjaman

(a) Warga Suruhanjaya yang ingin menggunakan peralatan ICT gunasama (*pool)* perlulah mengemukakan permohonan sama ada melalui memo/emel kepada Pengarah BPM selewat-lewatnya tiga (3) hari bekerja sebelum tarikh penggunaannya atas urusan rasmi Kerajaan.

(b) Warga Suruhanjaya yang ingin membuat peminjaman peralatan ICT perlu hadir ke BPM untuk mengisi borang KEW.PA-9 atau buku rekod sebelum dibenarkan untuk digunakan.

(c) Warga Suruhanjaya yang mengisi borang/buku rekod tersebut akan bertanggungjawab sepenuhnya terhadap peralatan ICT yang dipinjam.

(d) Warga Suruhanjaya yang membuat peminjaman perlu memulangkan semula peralatan ICT tersebut dalam keadaan lengkap, bersih dan sempurna dalam tempoh yang ditetapkan kepada BPM (pengesahan penghantaran dan penerimaan oleh pegawai yang dipertanggungjawabkan dan BPM).

(ii) Penjagaan dan Penyimpanan

(a) Peralatan ICT hendaklah sentiasa berada di bawah kawalan dan pengawasan warga Suruhanjaya Koperasi Malaysia yang dipertanggungjawabkan.

(b) Peralatan ICT perlu disimpan di dalam bilik khas/almari/ kabinet besi yang berkunci.

(c) Pegawai yang membuat pinjaman tersebut perlu mematuhi para 6.1

(d) Semua peralatan ICT gunasama (*pool*) hanya dibenarkan untuk penggunaan urusan rasmi Kerajaan/Suruhanjaya tertakluk kepada ketersediaan peralatan tersebut.

(c) Peralatan ICT gunasama (*pool*/Bahagian/Unit/Negeri/Wilayah)

(i) Peralatan ICT hendaklah sentiasa berada di bawah kawalan dan pengawasan Pegawai Aset Bahagian/Unit/Negeri/ Wilayah Suruhanjaya yang dipertanggungjawabkan.

(ii) Peralatan ICT perlu disimpan di dalam bilik khas/almari/ kabinet besi yang berkunci.

(iii) Komputer riba yang digunakan hendaklah sentiasa dikunci menggunakan *safety lock* yang telah dibekalkan oleh BPM (bagi Ibu Pejabat) dan IO Negeri (bagi Cawangan/Wilayah) sewaktu pengagihan/penerimaan peralatan tersebut.

(iv) Komputer riba yang tidak digunakan dalam tempoh masa yang lama tidak digalakkan diletakkan di atas meja sebaliknya hendaklah disimpan di dalam almari/kabinet besi yang berkunci.

(v) Komputer peribadi/komputer riba tidak boleh dibiarkan terletak di tempat yang terdedah kepada umum tanpa berkunci.

(vi) Semua peralatan ICT yang dipertanggungjawabkan (seperti pencetak, pengimbas) perlu disimpan/ditempatkan di lokasi yang selamat.

(vii) Semua peralatan ICT gunasama (*pool*) hanya dibenarkan untuk penggunaan urusan rasmi Kerajaan/Suruhanjaya Koperasi Malaysia sahaja dan perlu membuat pengisian borang KEW.PA-9.

(d) Penjagaan dan Penyimpanan Semasa di Rumah atau di Luar Pejabat.

(i) Peralatan ICT termasuk komputer tablet hendaklah disimpan di dalam almari yang berkunci.

(ii) Peralatan ICT termasuk komputer tablet tidak boleh dibiarkan terletak di tempat terbuka dan di mana-mana lokasi yang mudah dicapai seperti ruang tamu, atas meja makan, di tepi tingkap atau di tepi pintu setelah digunakan.

(iii) Semasa meninggalkan tempat kediaman/ tempat penginapan dan sebagainya, pengguna hendaklah memastikan bilik/ premis di mana Peralatan ICT termasuk komputer tablet disimpan berada dalam keadaan berkunci dan selamat.

(e) Penjagaan Semasa Menghadiri Program/Mesyuarat/ Kerja Luar/ Kursus/Seminar/Bengkel/Latihan/Persidangan dan lain-Lain atas urusan rasmi Kerajaan

(i) Sepanjang menghadiri program/mesyuarat/kerja luar/ kursus/ seminar/bengkel/latihan/persidangan dan lain-lain atas urusan rasmi Kerajaan, Peralatan ICT termasuk komputer tablet mestilah sentiasa berada di bawah kawalan sepenuhnya pegawai yang dipertanggungjawabkan.

(ii) Peralatan ICT yang ditinggalkan perlulah disimpan di dalam bilik/almari berkunci.

(iii) Peralatan ICT yang ditinggalkan di dalam bilik untuk program/mesyuarat/kerja luar/kursus/ seminar/bengkel/latihan/persidangan dan lain-lain yang berkaitan atas urusan rasmi Kerajaan, sekiranya berlaku kehilangan, ianya adalah di bawah tanggungjawab pegawai yang dipertanggungjawabkan.

(f) Penjagaan Semasa di dalam Kenderaan Individu atau Jabatan

(i) Peralatan ICT termasuk komputer tablet **tidak boleh ditinggalkan di dalam kenderaan** tanpa pengawasan.

(ii) Peralatan ICT termasuk komputer tablet perlu disimpan di dalam ruang penyimpanan kenderaan yang berkunci dan bukan di tempat yang mudah dilihat sekiranya pegawai meninggalkan kenderaan tanpa membawa peralatan tersebut.

(iii) Peralatan ICT termasuk komputer tablet yang dibawa dengan kenderaan lain seperti motosikal hendaklah di dalam bekas khas yang sentiasa selamat dan berkunci.

(iv) Peralatan ICT termasuk komputer tablet hendaklah sentiasa dilindungi dari pelbagai risiko kecurian atau kerosakan seperti terkena air (hujan/banjir dan sebagainya) atau dari haba tinggi (di bawah panas terik matahari).

7. PERTUKARAN PEGAWAI DAN LOKASI

7.1 Peralatan ICT

(a) Warga Suruhanjaya adalah bertanggungjawab untuk memulangkan kembali peralatan ICT ke BPM (bagi Ibu Pejabat) atau IO Negeri (bagi SKM Negeri/Wilayah) apabila bertukar ke Bahagian/ Unit/ SKM Negeri/SKM Wilayah/berhenti/bersara/tamat kontrak perkhidmatan/ bertukar keluar dari Suruhanjaya Koperasi Malaysia. Bagi peralatan ICT yang diklasifikasi sebagai aset Suruhanjaya, sebarang pertukaran penempatan hendaklah dimaklumkan kepada Pegawai Aset Bahagian dan Negeri (yang mana berkaitan) untuk dikemaskini dalam borang KEW.PA-7. Pegawai yang menerima hendaklah menyemak dan mengesahkan aset alih di penempatan tersebut.

(b) Walau bagaimana pun, dalam hal komputer tablet, warga Suruhanjaya adalah bertanggungjawab untuk memulangkan kembali komputer tablet tersebut kepada Pegawai Aset atau Setiausaha Pejabat (PA) atau Ketua Pembantu Tadbir (CC) Suruhanjaya Negeri dan Bahagian masing-masing serta

memaklumkan kepada BP Ibu Pejabat apabila bertukar ke Bahagian/Unit/Sektor/Seksyen lain/berhenti/ bersara/tamat kontrak perkhidmatan/bertukar keluar dari Suruhanjaya.

(c) Warga Suruhanjaya perlu memastikan semua maklumat Kerajaan di dalam peralatan ICT (komputer riba/komputer peribadi termasuk komputer tablet) telah dibuat salinan (*backup*) di peranti storan lain sebelum diserahkan kembali seperti klausa 7.1.

(d) Pegawai perlu memaklumkan kepada BPM untuk penyelarasan peralatan ICT sekiranya pegawai dinaikkan pangkat/bertukar ke Bahagian/Unit/Suruhanjaya Negeri/Suruhanjaya Wilayah/berhenti/ bersara/tamat kontrak perkhidmatan/bertukar keluar dari Suruhanjaya.

8. KEROSAKAN DAN PENYELENGGARAAN

8.1 Bagi warga Suruhanjaya di Ibu Pejabat, sebagai pengguna hendaklah segera melaporkan aduan kerosakan peralatan ICT sekiranya menghadapi masalah melalui Helpdesk ICT (https://rfs.skm.gov.my) atau emel ke bpminfra@skm.gov.my.

8.2 Bagi komputer tablet sewaan, warga Suruhanjaya hendaklah segera melaporkan aduan kerosakan tablet sekiranya tablet menghadapi masalah melalui Helpdesk pihak pembekal yang dilantik dengan merujuk pada stiker di bahagian belakang komputer tablet berkenaan.

8.3 Bagi warga Suruhanjaya di Negeri/Wilayah, aduan kerosakan peralatan ICT perlu dilaporkan melalui IO Negeri yang merupakan Pegawai yang bertanggungjawab untuk memaklumkan kepada Pembekal bagi tindakan selanjutnya. IO Negeri akan memaklumkan kepada BPM untuk pemantauan tempoh pembaikan berdasarkan kepada *Service Level Agreements* (SLA).

8.4 Aduan kerosakan bagi peralatan ICT yang diklasifikasikan sebagai aset Suruhanjaya perlu dilaporkan oleh warga Suruhanjaya di Negeri/ Wilayah, melalui IO Negeri yang merupakan Pegawai yang bertanggungjawab untuk memaklumkan kepada BPM bagi tindakan selanjutnya (semakan tempoh jaminan serta pandangan dari BPM sekiranya perlu). Aduan mengenai kerosakan Aset Alih hendaklah dilaporkan melalui Sistem Pengurusan Aset (SPA) atau menggunakan Borang Aduan Kerosakan Aset Alih KEW.PA-10.

KEW.PA-10 dan hendaklah mendapat kelulusan Ketua Jabatan sebelum penyelenggaraan dilaksanakan.

8.5 Sekiranya warga Suruhanjaya membawa keluar peralatan ICT sewaan termasuk komputer tablet dari lokasi pejabat Suruhanjaya, dan kemudian terlibat dengan kemalangan/banjir yang menyebabkan peralatan tersebut tersebut mengalami kerosakan atas kecuaian individu, adalah menjadi tanggungjawab pegawai tersebut untuk melaporkan kepada IO dan BPM (beserta dengan laporan polis/bukti kemalangan/pengesahan dari Ketua Jabatan) untuk sebarang tuntutan kepada pihak Pembekal.

8.6 Tanggungjawab warga Suruhanjaya yang dibekalkan dengan peralatan ICT termasuk komputer tablet serta aksesori perlu menggunakan aset tersebut dengan sebaik mungkin sepertimana keadaan sewaktu penerimaan.

8.7 Penyelenggaraan pencegahan (*preventive maintenance* (PM)) akan dilaksanakan oleh Pembekal mengikut jadual penyelenggaraan yang telah ditetapkan di dalam kontrak perjanjian sepanjang tempoh. Warga Suruhanjaya dikehendaki memberikan kerjasama sepanjang tempoh penyelenggaraan pencegahan dilakukan.

8.8 Sekiranya warga Suruhanjaya tidak membenarkan peralatan ICT termasuk komputer tablet diselenggara di atas faktor tertentu, mereka perlu memaklumkan kepada wakil Pembekal yang hadir untuk melaksanakan penyelenggaraan dan IO Negeri (SKM Negeri/Wilayah) atau BPM (Ibu Pejabat SKM) beserta justifikasi untuk rekod dan pemantauan BPM.

9. KEHILANGAN DAN KECURIAN

9.1 Tafsiran kehilangan bermaksud kehilangan peralatan ICT disebabkan oleh kecurian, kebakaran, kemalangan, bencana alam, kesusutan (kehilangan komponen peralatan ICT contoh memori, *hard disk* dan sebagainya), penipuan atau kecuaian warga Suruhanjaya.

9.2 Adalah menjadi tanggungjawab warga Suruhanjaya sebagai pengguna/ Ketua Jabatan atau IO untuk melaporkan segera sebarang kehilangan atau kecurian peralatan ICT di Balai Polis yang berhampiran.

9.3 Warga Suruhanjaya sebagai pengguna/Ketua Jabatan atau IO yang dipertanggungjawabkan perlu menyerahkan salinan laporan polis tersebut

kepada Pengarah BPM dan pihak pembekal dengan kadar segera. Bagi peralatan ICT di bawah kategori aset, pengurusan kehilangan aset adalah bawah peruntukan Tatacara Pengurusan Aset (TPA) Suruhanjaya Koperasi Malaysia.

9.4 Berikut adalah proses pengurusan kehilangan dan kecurian bagi peralatan ICT sewaan:

(a) Melapor Kehilangan

Apabila terdapat kehilangan peralatan ICT, tindakan yang perlu diambil adalah seperti berikut:

(i) Warga Suruhanjaya yang mengetahui kehilangan hendaklah melaporkannya kepada Ketua Jabatan dengan serta-merta.

(ii) Ketua Jabatan atau warga Suruhanjaya yang bertanggungjawab ke atas kehilangan atau yang mengetahui kehilangan berlaku, hendaklah membuat laporan polis dengan segera.

(iii) Laporan rasmi kehilangan perlu dilapor pada BPM oleh Ketua Jabatan atau Pegawai yang bertanggungjawab.

(b) Pegawai daripada BPM akan memaklumkan kehilangan peralatan ICT kepada BP untuk pelaksanaan Pelantikan Jawatankuasa Penyiasat.

(c) Melantik Jawatankuasa Penyiasat

(i) Jawatankuasa penyiasat hendaklah dilantik secara bertulis dalam tempoh dua (2) minggu.

(ii) Keanggotaan Jawatankuasa Penyiasat hendaklah terdiri daripada:

a. Pegawai yang tidak terlibat dengan kehilangan dan bukan dari bahagian/unit yang sama;

b. Sekurang-kurangnya dua (2) orang pegawai dan Ketuanya hendaklah daripada Kumpulan Pengurusan dan Profesional di gred yang bersesuaian; dan

c. Mempunyai pengalaman dalam pengurusan aset atau pengurusan kewangan jika perlu.

d. Bagi kes kehilangan yang berlaku di luar Malaysia, Pegawai Pengawal dibenarkan melantik pegawai bersesuaian dari Jabatan atau Agensi Kerajaan Malaysia lain yang tidak terlibat dengan kehilangan tersebut di negara berkenaan sebagai Jawatankuasa Penyiasat.

e. Bagi anggota keselamatan penubuhan Jawatankuasa Penyiasat adalah mengikut Akta atau Peraturan agensi keselamatan yang berkenaan.

f. Tugas dan tanggungjawab Jawatankuasa Penyiasat adalah untuk menjalankan siasatan dengan segera selepas perlantikan dengan mengambil tindakan berikut:

(i) Mengenal pasti pegawai yang bertanggungjawab ke atas kehilangan;

(ii) Menyoal siasat pegawai terlibat;

(iii) Melawat dan memeriksa tempat kejadian;

(iv) Mendapatkan bukti bergambar sekitar tempat kejadian, salinan dokumen yang berkaitan sebagai bahan bukti.

(v) Selepas pelaksanaan tugas selesai dan semua bukti telah dapat dikumpul, penyediaan laporan akhir perlu dilaksanakan.

Carta Alir proses adalah seperti di **Lampiran D**.

9.5 Berdasarkan kepada laporan hasil siasatan dan cadangan tindakan susulan oleh Jawatankuasa Penyiasat yang dilantik, Pengerusi Eksekutif

berhak menentukan sama ada kehilangan ini disebabkan kecuaian pegawai atau sebaliknya.

9.6 Sekiranya terdapat unsur kecuaian, BPM dan pihak pembekal akan memaklumkan nilai ganti rugi yang perlu dibayar oleh warga Suruhanjaya yang bertanggungjawab atas kehilangan atau kecurian peralatan ICT tersebut.

9.7 Pihak pembekal akan menggantikan peralatan ICT sewaan yang baharu kepada warga Suruhanjaya tersebut selepas bayaran ganti rugi dilaksanakan.

9.8 Sekiranya selepas siasatan dilakukan dan didapati tiada unsur kecuaian, pihak pembekal akan menggantikan terus peralatan ICT yang baharu kepada warga Suruhanjaya tersebut.

9.9 Tindakan tatatertib di bawah Akta Badan-Badan Berkanun 2000 - (Tatatertib dan Surcaj) boleh dikenakan ke atas warga Suruhanjaya yang sengaja menyebabkan kerosakan/kehilangan/penyelewangan/salah guna peralatan ICT dan sengaja menyebabkan kerugian kepada Kerajaan.

9.10 Kemudahan ICT juga boleh dilucutkan jika penggunaannya melanggar Aku Janji.

10. PEMAKAIAN DAN TARIKH KUAT KUASA

Semua warga Suruhanjaya hendaklah mematuhi garis panduan ini untuk memastikan pelaksanaan kemudahan penyampaian ICT khususnya perkhidmatan peralatan ICT dapat berjalan dengan lancar dan memenuhi keperluan urusan rasmi Kerajaan. Pemakaian Garis Panduan Dalaman ini berkuatkuasa serta merta.

(HAJI ZAZALI BIN HARON)
PENGERUSI EKSEKUTIF

TARIKH : 5/4/2022

GLOSARI

Pegawai Dipertanggungjawabkan	- Pemegang Unit Peralatan aset atau sewaan ICT
Warga Suruhanjaya	- *Pegawai dan kakitangan di Suruhanjaya Koperasi Malaysia yang berstatus jawatan Tetap, Kontrak, Pekerja Sambilan Harian (PSH), Praktikal/ Latihan Industri dan pegawai pinjaman dari luar.*
Pengarah Negeri	- Pengarah Suruhanjaya Cawangan Negeri.
Peralatan ICT	- Merangkumi perolehan aset atau sewaan.
Ketua Jabatan	Pengerusi Eksekutif/Timbalan Pengerusi Eksekutif/Naib Pengerusi Eksekutif/Pengarah Bahagian/Pengarah Negeri.
Pegawai IO	- Pegawai yang dipertanggunjawabkan untuk membantu BPM mengendalikan Peralatan ICT. Tugas IO seperti di **Lampiran E**.

LAMPIRAN A

AKU JANJI PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN/KOMPUTER TABLET (*) BAGI IBU PEJABAT

[(*) Sila potong yang mana tidak berkaitan]

SURUHANJAYA KOPERASI Malaysia

AKU JANJI PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN/KOMPUTER TABLET(*) BAGI IBU PEJABAT
[(*) Sila potong yang mana tidak berkaitan]

Saya, ... No. K/P : ..... yang bertugas di Suruhanjaya Ibu Pejabat di Bahagian/Unit ....., dengan ini mengaku telah menerima peralatan sewaan peralatan ict sewaan/komputer tablet (*) seperti mana di dalam Jadual pada ..... bagi tujuan tugasan rasmi Suruhanjaya sahaja.

Saya juga akan bertanggungjawab ke atas keselamatan peralatan sewaan tersebut dengan memastikan peralatan berkenaan disimpan di tempat yang selamat dan sentiasa di bawah kawalan saya dan saya akur untuk dikenakan tindakan bayaran balik, penggantian atau tatatertib jika berlaku kerosakan, kecurian atau penipuan disebabkan kecuaian saya terhadap peralatan sewaan.

Sekiranya saya tidak lagi berkhidmat di Suruhanjaya/cuti panjang, maka peralatan sewaan tersebut akan diserahkan semula kepada Pengarah Bahagian Pengurusan Maklumat atau Bahagian Pentadbiran (dalam hal komputer tablet) SKM Ibu Pejabat berserta dengan Borang Pemulangan Sewaan Peralatan ICT seperti di **Borang A**. Peralatan dan aksesori ICT hendaklah **DIPULANGKAN** kepada BPM atau BP (yang mana berkaitan) jika bersara, berhenti dan bertukar ke negeri dan wilayah. Peralatan dan aksesori ini telah didaftarkan untuk pegawai bertugas di **Ibu pejabat Negeri** Suruhanjaya **SAHAJA**.

Suruhanjaya berhak menarik balik peralatan sewaan yang telah diserahkan kepada saya, jika saya tidak mematuhi Dasar Keselamatan ICT Kerajaan (Pekeliling Am Bilangan 3 Tahun 2000) dan Tatacara Pengurusan Aset Suruhanjaya Koperasi Malaysia.

Panduan penggunaan, penjagaan dan penyimpanan peralatan sewaan ICT adalah seperti di lampiran.

Tandatangan Penerima		Disahkan Oleh	
..... Nama	:	..... Nama	:
		Jawatan	:
Jawatan	:	Tarikh	:
Tarikh	:		
No Tel	:		

Nota: Hanya penerima sahaja dibenarkan menandatangani borang Aku Janji ini. Wakil/bagi pihak tidak dibenarkan

BORANG PEMULANGAN PERALATAN ICT SEWAAN

Borang A

SURUHANJAYA KOPERASI Malaysia	**BORANG PEMULANGAN SEWAAN PERALATAN ICT** **Pengarah Bahagian Pengurusan Maklumat** **Suruhanjaya Koperasi Malaysia** **Menara Suruhanjaya Koperasi Malaysia, Changkat Semantan,** **Off Jalan Semantan, Bukit Damansara, 50490 Kuala Lumpur**

BAHAGIAN A: MAKLUMAT PEGAWAI YANG MENYERAHKAN PERALATAN	
Nama	
Jawatan / Gred	
Ibu Pejabat / Negeri	
Bahagian / Wilayah	
Email	
No. Tel Pejabat / Bimbit	

Tujuan Pemulangan: Berhenti Bersara Cuti Panjang Lain-lain (nyatakan):

BAHAGIAN B: MAKLUMAT ASET ICT

	MAKLUMAT ASET / ALATAN TAMBAHAN	NOMBOR SIRI PEMBUATAN

BAHAGIAN C: PERAKUAN PENYERAHAN

Saya dengan ini mengakui telah:

1. **Memulangkan aset dalam keadaan yang sempurna tanpa sebarang kerosakan**
2. **Memulangkan aset bersama semua aksesori yang disertakan.**

Tandatangan : .....
Tarikh Serahan :

BAHAGIAN D: PERAKUAN PENERIMAAN (DIISI OLEH BPM)

Tandatangan & Cop Penerima : .....

Nama :
Tarikh :

BAHAGIAN E: CATATAN BPM

Saya telah memeriksa dan menyemak setiap alatan dan didapati : Lengkap
Rosak Hilang : Nyatakan Lain-lain : Nyatakan

.....
Tandatangan Tarikh :
Nama & Cop

BORANG PEMULANGAN KOMPUTER TABLET

Borang A1

SURUHANJAYA KOPERASI Malaysia	**BORANG PEMULANGAN KOMPUTER TABLET** **Pengarah Bahagian Pentadbiran** **Suruhanjaya Koperasi Malaysia** **Menara Suruhanjaya Koperasi Malaysia, Changkat Semantan,** **Off Jalan Semantan, Bukit Damansara, 50490 Kuala Lumpur**

BAHAGIAN A: MAKLUMAT PEGAWAI YANG MENYERAHKAN PERALATAN	
Nama	
Jawatan / Gred	
Ibu Pejabat / Negeri	
Bahagian / Wilayah	
Email	
No. Tel Pejabat / Bimbit	
Tujuan Pemulangan: Berhenti Bersara Cuti Panjang Lain-lain (nyatakan):	

BAHAGIAN B: MAKLUMAT ASET ICT		
	MAKLUMAT ASET / ALATAN TAMBAHAN	**NOMBOR SIRI PEMBUATAN**

BAHAGIAN C: PERAKUAN PENYERAHAN

Saya dengan ini mengakui telah:

1. **Memulangkan aset dalam keadaan yang sempurna tanpa sebarang kerosakan**
2. **Memulangkan aset bersama semua aksesori yang disertakan.**

Tandatangan : .....
Tarikh Serahan :

BAHAGIAN D: PERAKUAN PENERIMAAN (DIISI OLEH BP)

Tandatangan & Cop Penerima : .....
Nama :
Tarikh :

BAHAGIAN E: CATATAN BP

Saya telah memeriksa dan menyemak setiap alatan dan didapati : Lengkap
Rosak Hilang : Nyatakan Lain-lain : Nyatakan

.....
Tandatangan Tarikh :
Nama & Cop

JADUAL PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN

IBU PEJABAT
Lampiran A

JADUAL PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN SURUHANJAYA KOPERASI MALAYSIA

MAKLUMAT ASET ICT		
BIL.	**MAKLUMAT ASET / ALATAN**	**NOMBOR SIRI PEMBUATAN**
1	MODEL :	
2	NO SIRI :	
3	NO. SIRI ADAPTER	
4	BACKPACK	
5	NO. SIRI USB OPTICAL MOUSE	
6	DOCKING STATION CABLE LOCK	
7	NO. SIRI NUMERIC KEY	
8	NO. SIRI HDMI TO VGA	
9	NO. SIRI USB TYPE C RJ45	

PERAKUAN PENERIMAAN

Tandatangan Penerima

.....
Nama :
Jawatan :
Tarikh :

Disahkan Oleh BPM

.....
Nama :
Jawatan :
Tarikh :

PANDUAN PENGGUNAAN, PENJAGAAN DAN PENYIMPANAN PERALATAN ICT SEWAAN

Lampiran B

PANDUAN PENGGUNAAN, PENJAGAAN DAN PENYIMPANAN PERALATAN ICT SEWAAN SURUHANJAYA KOPERASI MALAYSIA

1. Peraturan penggunaan peralatan ICT hendaklah mematuhi Tatacara Pengurusan Aset Suruhanjaya Koperasi Malaysia seperti berikut:

(a) digunakan bagi tujuan rasmi sahaja;

(b) digunakan bagi mengikut fungsi sebenar seperti yang terdapat dalam manual/buku panduan pengguna mengikuti garis panduan Dasar Keselamatan ICT;

(c) dikendalikan oleh pegawai yang mahir dan berkelayakan;

(d) melaporkan aduan kerosakan peralatan ICT segera kepada pihak pembekal dan Bahagian Pengurusan maklumat untuk tindakan seterusnya; dan

(e) sebarang kehilangan aset, peralatan ICT dan aksesori adalah merupakan tanggungjawab pegawai yang terlibat.

2. Peraturan penjagaan dan penyimpanan peralatan ICT yang perlu diberi penekanan adalah seperti berikut:

2.1 Penjagaan dan Penyimpanan Semasa di Pejabat

(a) Peralatan ICT hendaklah sentiasa berada di bawah pengawasan pegawai. Pegawai perlu mengunci peralatan ICT menggunakan *Docking Station Cable Lock Notebook* yang telah dibekalkan.

(b) Peralatan ICT hendaklah disimpan di dalam tempat yang selamat.

(c) Peralatan ICT tidak boleh dibiarkan terletak di tempat yang terdedah kepada umum.

2.2 Penjagaan dan Penyimpanan Semasa di Rumah

(a) Peralatan ICT hendaklah disimpan di dalam almari/ kabinet yang berkunci.

(b) Peralatan ICT setelah digunakan tidak boleh dibiarkan terletak di ruang tamu, di atas meja makan atau di tepi pintu.

(c) Semasa meninggalkan rumah, pengguna hendaklah memastikan bilik di mana peralatan ICT disimpan dan rumah berada dalam keadaan berkunci dan selamat.

2.3 Penjagaan Semasa Menghadiri Program/Mesyuarat/Kerja Luar/ Kursus/Seminar/Bengkel/Latihan/Persidangan dan lain-lain atas urusan rasmi Kerajaan

(a) Semasa menghadiri kerja luar/kursus/seminar/bengkel, semua peralatan ICT mesti dibawa bersama pengguna.

(b) Jika tidak digunakan, peralatan ICT hendaklah ditinggalkan di dalam bilik seminar/bilik penginapan yang berkunci dengan selamat.

2.4 Penjagaan Semasa di dalam Kenderaan

Peralatan ICT **TIDAK BOLEH** ditinggalkan di dalam kenderaan tanpa pengawasan.

2.5 Penjagaan Kebersihan Peralatan ICT

Peralatan dan Aksesori hendaklah dijaga dengan baik dan sentiasa berada dalam keadaan yang bersih dan sempurna seperti mana semasa ianya diterima oleh pegawai.

2.6 Pemulangan Peralatan ICT

Peralatan dan Aksesori ICT hendaklah DIPULANGKAN kepada BPM atau BP (yang mana berkaitan) jika bersara, berhenti dan bertukar ke negeri dan wilayah. **Peralatan dan Aksesori ini telah didaftarkan untuk pegawai bertugas di Ibu Pejabat MENARA SKM SAHAJA.**

LAMPIRAN B

REKOD PERGERAKAN PERALATAN ICT SEWAAN

Siri Pembuatan _____

SURUHANJAYA KOPERASI Malaysia

REKOD PERGERAKAN PERALATAN SEWAAN ICT

Kementerian/ Jabatan : **IBU PEJABAT SURUHANJAYA KOPERASI MALAYSIA**
Bahagian : **BAHAGIAN PENGURUSAN MAKLUMAT**

MAKLUMAT PEROLEHAN	
Pembekal	
Kontrak Sewaan	
Tempoh Sewaan	
MAKLUMAT PERALATAN	
Kategori	
Sub Kategori	
Jenis/Jenama/Model	
No. Casis/ Siri Pembuat	
KOMPONEN/AKSESORI	
Smart AC adapter	
HP Business Backpack	
HP USB Optical Mouse	
Cable Lock Notebook	

PENEMPATAN				
Lokasi				
Tarikh				
Nama Pegawai				
Tandatangan				

LAMPIRAN C

AKU JANJI PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN

SKM NEGERI DAN WILAYAH
AKU JANJI PENERIMAAN DAN PENGGUNAAN PERALATAN ICT
SEWAAN SURUHANJAYA KOPERASI MALAYSIA

Saya, ... No. K/P : ..... yang bertugas di Suruhanjaya Koperasi Malaysia. Negeri/ Wilayah....., dengan ini telah menerima peralatan sewaan seperti mana di dalam Jadual di **Lampiran A** pada ..... bagi tujuan tugasan rasmi Suruhanjaya sahaja.

Saya juga akan bertanggungjawab ke atas keselamatan peralatan sewaan tersebut dengan memastikan peralatan berkenaan disimpan di tempat yang selamat dan sentiasa di bawah kawalan saya dan saya akur untuk dikenakan tindakan bayaran balik, penggantian atau tatatertib jika berlaku kerosakan, kecurian atau penipuan disebabkan kecuaian saya terhadap peralatan sewaan.

Sekiranya saya tidak lagi berkhidmat di Suruhanjaya / cuti panjang, maka peralatan sewaan tersebut akan diserahkan semula kepada Pengarah SKM Negeri dan mengemaskini rekod penempatan kepada Pegawai IO Negeri berserta dengan Borang Pemulangan Sewaan Peralatan ICT seperti di **Borang A**.

Suruhanjaya berhak menarik balik peralatan sewaan yang telah diserahkan kepada saya, jika saya tidak mematuhi Dasar Keselamatan ICT Kerajaan (Pekeliling Am Bilangan 3 Tahun 2000) dan Tatacara Pengurusan Aset Suruhanjaya Koperasi Malaysia.

Panduan penggunaan, penjagaan dan penyimpanan peralatan sewaan ICT adalah seperti di **Lampiran B**.

Tandatangan Penerima	Disahkan Oleh
.....	.....
Nama :	Nama :
Jawatan :	Jawatan :
Tarikh :	Tarikh :
No Tel :	

Nota : Hanya penerima sahaja dibenarkan menandatangani borang Aku Janji ini. Wakil/bagi pihak tidak dibenarkan

BORANG PEMULANGAN SEWAAN PERALATAN ICT SEWAAN

Borang A

SURUHANJAYA KOPERASI Malaysia	**BORANG PEMULANGAN SEWAAN PERALATAN ICT** **PENGARAH SKM NEGERI ( )**

BAHAGIAN A: MAKLUMAT PEGAWAI YANG MENYERAHKAN PERALATAN	
Nama	
Jawatan / Gred	
Ibu Pejabat / Negeri	
Bahagian / Wilayah	
Email	
No. Tel Pejabat / Bimbit	
Tujuan Pemulangan: Berhenti Bersara Cuti Panjang Lain-lain (nyatakan):	

BAHAGIAN B: MAKLUMAT ASET ICT

	MAKLUMAT ASET / ALATAN	NOMBOR SIRI PEMBUATAN

BAHAGIAN C: PERAKUAN PENYERAHAN

Saya dengan ini mengakui telah:

1. **Memulangkan aset dalam keadaan yang sempurna tanpa sebarang kerosakan**
2. **Memulangkan aset bersama semua aksesori yang disertakan.**

Tandatangan : .....

BAHAGIAN D: PERAKUAN PENERIMAAN (DIISI OLEH PEGAWAI IO NEGERI)

Tandatangan & Cop Penerima : .....
Nama :

BAHAGIAN E: CATATAN PEGAWAI IO NEGERI

Saya telah memeriksa dan menyemak setiap alatan dan didapati : Lengkap
Rosak
Hilang : Nyatakan Lain-lain : Nyatakan

.....
Tandatangan
Nama & Cop

Tarikh :

JADUAL PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN

Lampiran A

JADUAL PENERIMAAN DAN PENGGUNAAN PERALATAN ICT SEWAAN SURUHANJAYA KOPERASI MALAYSIA

MAKLUMAT ASET ICT		
BIL	**MAKLUMAT ASET / ALATAN**	**NOMBOR SIRI**
1	Model	
2	No. Siri AC adapter	
3	Business Backpack	
4	No. Siri USB Optical Travel Mouse	
5	No. Siri Docking Station Cable Lock	
6	No. Siri Numeric Key	

PERAKUAN PENERIMAAN

Tandatangan Penerima

.....
Nama :
Jawatan :
Tarikh :

Disahkan Oleh

.....
Nama :
Jawatan :
Tarikh :

PANDUAN PENGGUNAAN, PENJAGAAN DAN PENYIMPANAN PERALATAN ICT SEWAAN

SKM NEGERI DAN WILAYAH
Lampiran B

PANDUAN PENGGUNAAN, PENJAGAAN DAN PENYIMPANAN PERALATAN ICT SEWAAN SURUHANJAYA KOPERASI MALAYSIA

1. **Peraturan penggunaan peralatan ICT hendaklah mematuhi Tatacara Pengurusan Aset Suruhanjaya Koperasi Malaysia seperti berikut :**

   (a) digunakan bagi tujuan rasmi sahaja;

   (b) digunakan bagi mengikut fungsi sebenar seperti yang terdapat dalam manual/ buku panduan pengguna mengikuti garis panduan Dasar Keselamatan ICT;

   (c) dikendalikan oleh pegawai yang mahir dan berkelayakan;

   (d) melaporkan aduan kerosakan peralatan ICT segera kepada pihak pembekal dan Bahagian Pengurusan maklumat untuk tindakan seterusnya; dan

   (e) sebarang kehilangan aset, peralatan ICT dan aksesori adalah merupakan tanggungjawab pegawai yang terlibat.

2. **Peraturan penjagaan dan penyimpanan peralatan ICT yang perlu diberi penekanan adalah seperti berikut :**

   2.1 Penjagaan dan Penyimpanan Semasa di Pejabat

   (a) Peralatan ICT hendaklah sentiasa berada di bawah pengawasan pegawai. Pegawai perlu mengunci peralatan ICT menggunakan *Docking Station Cable Lock Notebook* yang telah dibekalkan.

   (b) Peralatan ICT hendaklah disimpan di dalam tempat yang selamat.

   (c) Peralatan ICT tidak boleh dibiarkan terletak di tempat yang terdedah kepada umum.

2.2 Penjagaan dan Penyimpanan Semasa di Rumah

(a) Peralatan ICT hendaklah disimpan di dalam almari/ kabinet yang berkunci.

(b) Peralatan ICT setelah digunakan tidak boleh dibiarkan terletak di ruang tamu, di atas meja makan atau di tepi pintu.

(c) Semasa meninggalkan rumah, pengguna hendaklah memastikan bilik di mana peralatan ICT disimpan dan rumah berada dalam keadaan berkunci dan selamat.

2.3 Penjagaan Semasa Menghadiri Program/ Mesyuarat/Kerja Luar/ Kursus/Seminar/Bengkel/Latihan/Persidangan dan lain-lain atas urusan rasmi Kerajaan

(a) Semasa menghadiri kerja luar/kursus/seminar/bengkel, semua peralatan ICT mesti dibawa bersama pengguna.

(b) Jika tidak digunakan, peralatan ICT hendaklah ditinggalkan di dalam bilik seminar/ bilik penginapan yang berkunci dengan selamat.

2.4 Penjagaan Semasa di dalam Kenderaan

Peralatan ICT TIDAK BOLEH ditinggalkan di dalam kenderaan tanpa pengawasan.

2.5 Penjagaan Semasa di dalam Kenderaan

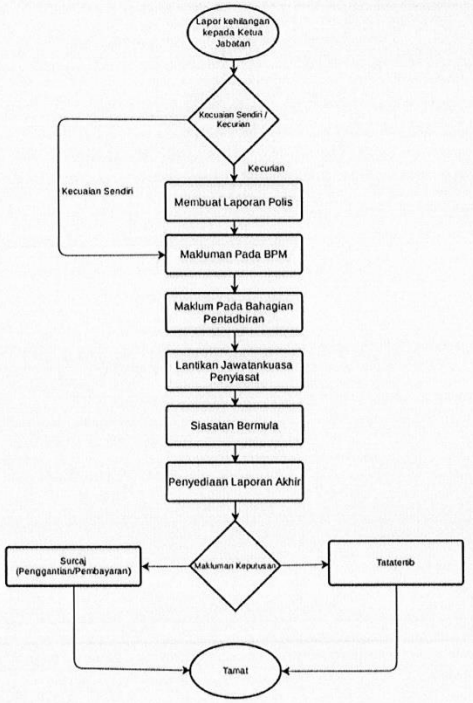
Peralatan **ICT TIDAK BOLEH** ditinggalkan di dalam kenderaan tanpa pengawasan.

2.6 Penjagaan Kebersihan Peralatan ICT

Peralatan dan Aksesori hendaklah dijaga dengan baik dan sentiasa berada dalam keadaan yang bersih dan sempurna seperti mana semasa ianya diterima oleh pegawai.

LAMPIRAN D

CARTA ALIR PROSES PENGURUSAN KEHILANGAN DAN KECURIAN BAGI PERALATAN ICT



LAMPIRAN E

TUGAS/TANGGUNGJAWAB PEGAWAI MAKLUMAT (IO)

1. Membantu Bahagian Pengurusan Maklumat (BPM) merancang aktiviti pelaksanaan Sistem Maklumat Suruhanjaya Ibu Pejabat dan Cawangan Suruhanjaya

2. Memastikan komputer dan peralatannya serta sistem yang digunakan di Suruhanjaya dapat beroperasi dengan baik. Memastikan pegawai membuat *clean-up* pada server (IO Cawangan) dan juga pengguna secara berkala bagi menjimatkan ruang storan komputer.

3. Menghubungi pihak berkaitan sekiranya berlaku kerosakan pada perisian dan perkakasan komputer.

4. Bersedia membantu pegawai/kakitangan yang menghadapi masalah dalam penggunaan komputer terutamanya yang berkaitan dengan sistem Suruhanjaya.

5. Bertindak sebagai tenaga pengajar/orang yang bertanggungjawab memberi latihan dan tunjuk ajar tentang penggunaan dalam sistem yang digunakan di Suruhanjaya.

6. Bertanggungjawab menjaga (*maintain*)/menentukan kesahihan data yang dimasukkan dalam sistem yang digunakan di Suruhanjaya

7. Membantu membuat repair dan recovery database ketika *database down* (sekiranya perlu)

8. Membaiki kerosakan kecil pada komputer dan peralatannya (*troubleshooting*) sama ada dari segi perisian dan perkakasan.

9. Menyediakan laporan yang diperlukan oleh pihak pengurusan yang berkaiitan dengan perjalanan system dan data tertentu.

10. Membantu menyelaras program Latihan ICT Cawangan

LAMPIRAN F

BIDANG TUGAS PENGURUSAN ICT KATEGORI TABLET

1. Bahagian Pengurusan Maklumat akan mengesahkan spesifikasi tablet termasuk aksesori sekiranya terdapat penerimaan, pertukaran dan pemulangan, termasuk melaksanakan konfigurasi yang berkaitan (email, *reset password*, dan lain-lain).

2. Pengagihan bagi komputer tablet kepada mana-mana warga Suruhanjaya yang berkelayakan akan dilaksanakan oleh Bahagian Pentadbiran (BP).

3. Bahagian Pengurusan Maklumat akan menerima dan mengesahkan borang penerimaan UAT dan agihan komputer tablet dan akan menyalurkan maklumat kepada Bahagian Pentabiran untuk penyelarasan dan simpanan rekod.

4. Bahagian Pengurusan Maklumat akan menerima borang pemulangan dan menyalurkan rekod kepada Bahagian Pentadbiran. Bahagian Pentadbiran bertanggungjawab untuk menguruskan dan mengemaskini rekod pengguna dari semasa ke semasa.

5. Bagi kes kehilangan, Bahagian Pengurusan Maklumat akan menerima laporan kehilangan awal daripada Bahagian, Negeri atau Pusat Tanggungjawab (PTJ) dan akan menyalurkan kepada Bahagian Pentadbiran untuk tindakan selanjutnya.

6. Untuk urusan kerosakan pengguna boleh memaklumkan kepada pihak pembekal untuk pelaksanaan aktiviti *preventive* serta *corrective maintenance* serta memaklumkan kepada Bahagian Pentadbiran bagi polisi perjanjian.

7. Sebarang urusan pembayaran, penyediaan kontrak, dan segala yang berkaitan tentang ikatan liabiliti antara Suruhanjaya dengan pembekal adalah diuruskan oleh Bahagian Pentadbiran.

8. Bahagian Pentadbiran dan Bahagian Pengurusan Maklumat mempunyai hak untuk mengambil/ menyimpan komputer tablet jika perlu.

LAMPIRAN 3

GARIS PANDUAN MENGENAI PENGAGIHAN PERALATAN ICT

SURUHANJAYA KOPERASI MALAYSIA

LAMPIRAN 3: GARIS PANDUAN MENGENAI PENGAGIHAN PERALATAN ICT

SURUHANJAYA KOPERASI Malaysia

GARIS PANDUAN MENGENAI PENGAGIHAN PERALATAN ICT DI SURUHANJAYA KOPERASI MALAYSIA

1. PENGENALAN

1.1 Tujuan garis panduan ini diwujudkan bagi menjelaskan dasar berkaitan pengagihan peralatan ICT di Suruhanjaya Koperasi Malaysia. Ia merangkumi perkara-perkara berikut:

a) Garis panduan ini diguna pakai di Ibu Pejabat SKM, SKM Negeri, Wilayah dan PULAKOP.

b) Kelayakan pengagihan peralatan ICT bagi pegawai dan kakitangan Suruhanjaya Koperasi Malaysia.

c) Kuasa yang meluluskan bagi pengagihan dibuat.

d) Semua peralatan ICT tanpa mengira punca perolehan adalah tertakluk kepada garis panduan ini.

e) Penempatan aset kekal di lokasi sedia ada.

Kumpulan sasaran bagi garis panduan ini adalah semua pegawai dan kakitangan di Suruhanjaya Koperasi Malaysia yang berstatus jawatan Tetap, Kontrak, Pekerja Sambilan Harian (PSH), Pegawai Khas, Praktikal / Latihan Industri dan pegawai pinjaman dari luar.

2. LATAR BELAKANG

2.1 Infrastruktur Teknologi Maklumat dan Komunikasi (ICT) merupakan elemen penting yang terkandung di dalam Pelan Perancangan Strategik Teknologi Maklumat dan Komunikasi (PSTMK), Suruhanjaya Koperasi Malaysia. Salah satu objektif utama Bahagian Pengurusan Maklumat yang dinyatakan dalam PSTMK adalah bertanggungjawab untuk memastikan

sumber-sumber ICT disediakan dan digunakan secara optimum bagi meningkatkan kecekapan perkhidmatan pentadbiran.

2.2 Bahagian Pengurusan Maklumat merupakan bahagian yang dipertanggungjawabkan untuk menguruskan pengagihan peralatan ICT bagi Ibu Pejabat Suruhanjaya Koperasi Malaysia.

2.3 Pengarah Negeri dipertanggungjawabkan untuk menguruskan pengagihan peralatan ICT bagi Negeri/ Wilayah.

2.4 Penyelarasan dan penyeragaman pengagihan peralatan ICT bertujuan untuk mengelakkan pembaziran sumber dan menjimatkan kos serta memudahkan kerja-kerja penyelenggaraan.

3. KELAYAKAN UNTUK PENGAGIHAN

Kelayakan pengagihan peralatan ICT hendaklah dilaksanakan mengikut kaedah pengagihan seperti berikut:

3.1 Pengagihan Mengikut Jawatan

3.1.1 Pengerusi Eksekutif/ Timbalan Pengerusi Eksekutif/ Naib Pengerusi Eksekutif

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*; atau satu (1) unit *notebook*	Mengikut keperluan
ii.	Satu (1) unit pencetak *laser* peribadi	

3.1.2 Pengarah/ Timbalan Pengarah

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*; atau satu (1) unit *notebook*	Mengikut keperluan
ii.	Satu (1) unit pencetak *laser* peribadi	Bagi Pengarah dan Timbalan Pengarah gred 48 dan ke atas.

3.1.3 Gred 41 hingga Gred 48

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*; atau satu (1) unit *notebook*	Mengikut keperluan
ii.	Bagi gred 48 Satu (1) unit pencetak *laser* peribadi	
iii.	Bagi Gred 41 dan Gred 44 Satu (1) unit pencetak *laser* rangkaian berpusat dikongsi minimum 2 pegawai	Bergantung kepada faktor keperluan seperti kedudukan pegawai dan beban tugas cetakan

* Nota : Pengagihan satu (1) unit pencetak *laser* peribadi mengikut keperluan norma kerja boleh diberikan kepada pegawai Gred 41 hingga Gred 48. Norma kerja yang sesuai untuk dipertimbangkan dalam pengagihan pencetak *laser* peribadi adalah seperti berikut:

i. Menguruskan pencetakan dokumen dan laporan terperingkat; dan
ii. Menguruskan pencetakan pesanan kerajaan, baucar dan lain-lain.

3.1.4 Gred 27 hingga Gred 38

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*; atau satu (1) unit *notebook*	Mengikut keperluan
ii.	Satu (1) unit pencetak *laser* rangkaian berpusat dikongsi minimum 3 pegawai	Bergantung kepada faktor keperluan seperti kedudukan pegawai dan beban tugas cetakan

* Nota : Pengagihan satu (1) unit pencetak *laser* peribadi mengikut keperluan norma kerja boleh diberikan kepada pegawai Gred 27 hingga Gred 38. Norma kerja yang sesuai untuk dipertimbangkan dalam pengagihan pencetak *laser* peribadi adalah seperti berikut:

i. Menguruskan pencetakan dokumen dan laporan terperingkat;
ii. Menguruskan pencetakan pesanan kerajaan, baucar dan lain-lain; dan
iii. Melakukan tugasan khas seperti Pembantu Peribadi (PA).

3.1.5 Gred 26 dan ke bawah

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*	Mengikut keperluan
ii.	Satu (1) unit pencetak *laser* rangkaian berpusat dikongsi minimum 5 pegawai.	Bergantung kepada faktor keperluan seperti kedudukan pegawai dan beban tugas cetakan

* Nota : Pengagihan satu (1) unit pencetak *laser* peribadi mengikut keperluan norma kerja boleh diberikan kepada pegawai Gred 26 dan ke bawah. Norma kerja yang sesuai untuk dipertimbangkan dalam pengagihan pencetak *laser* peribadi adalah seperti berikut:

i. Menguruskan pencetakan dokumen dan laporan terperingkat;
ii. Menguruskan pencetakan pesanan kerajaan, baucar dan lain-lain; dan
iii. Melakukan tugasan khas seperti Pembantu Peribadi (PA).

3.1.6 Pegawai Gunasama

Pengagihan peralatan ICT sama seperti Gred di atas.

3.1.7 Pegawai khas / Kontrak, Pekerja Sambilan Harian (PSH) / Praktikal / Latihan Industri / Pegawai pinjaman dari luar

Bil	Keterangan	Catatan
i.	Satu (1) unit komputer *desktop*	
ii.	Satu (1) unit pencetak *laser* peribadi; atau satu (1) unit pencetak *laser* rangkaian berpusat dikongsi minimum 3 pegawai	Bergantung kepada faktor keperluan seperti kedudukan

Bil	Keterangan	Catatan
		pegawai dan beban tugas cetakan

* Nota : Pengagihan satu (1) unit pencetak *laser* peribadi mengikut keperluan norma kerja boleh diberikan kepada pegawai Gred 26 dan ke bawah. Norma kerja yang sesuai untuk dipertimbangkan dalam pengagihan pencetak *laser* peribadi adalah seperti berikut:

i. Menguruskan pencetakan dokumen dan laporan terperingkat;
ii. Menguruskan pencetakan pesanan kerajaan, baucar dan lain-lain; dan
iii. Melakukan tugasan khas seperti Pembantu Peribadi (PA).

3.2 Pengagihan Mengikut Jenis Peralatan

Bil	Peralatan	Keterangan
i.	Komputer *desktop*	Satu (1) unit komputer *desktop* dipertimbangkan untuk diagihkan di Bilik Mesyuarat Utama.
ii.	*Notebook*	*Notebook* gunasama di BPM dan Negeri untuk kegunaan majlis rasmi/ mesyuarat/ kursus/ bengkel/ kerja luar.
iii.	Pencetak *laser* warna	Satu (1) unit pencetak *laser* warna dipertimbangkan untuk diberikan kepada bahagian mengikut keperluan. Pengagihan bergantung kepada mesin fotostat rangkaian sedia ada yang mempunyai kemudahan mencetak warna.
iv.	Projektor	i. Satu (1) unit projektor dipasang di setiap Bilik Mesyuarat Utama dan Bilik Mesyuarat Utama Bahagian.

Bil	Peralatan	Keterangan
		ii. Projektor gunasama di BPM dan Negeri untuk kegunaan majlis rasmi/ mesyuarat/ kursus/ bengkel/ kerja luar.
v.	*External Drive & Pendrive*	i. Akan dipertimbangkan mengikut permohonan dan stok

4. KUASA YANG MELULUS PENGAGIHAN

Kuasa meluluskan pengagihan peralatan ICT ini terletak kepada Pengarah Bahagian Pengurusan Maklumat/ Pengarah Negeri melalui permohonan peralatan ICT yang dibuat.

5. PUNCA PEROLEHAN

Semua peralatan ICT tanpa mengira punca perolehan adalah tertakluk kepada garis panduan ini.

6. PENEMPATAN ASET ICT

Sekiranya berlaku perubahan struktur organisasi atau perpindahan pegawai, penempatan aset perlu dikekalkan di SKM Ibu Pejabat/ SKM Negeri untuk kegunaan pegawai baru. Sekiranya terdapat keperluan untuk memindahkan peralatan ICT, kelulusan dari Bahagian Pengurusan Maklumat / Pengarah Negeri perlu diperolehi.

7. PENUTUP

Garis panduan pengagihan peralatan ICT ini akan menjadi sumber rujukan utama dalam menguruskan pengagihan perkakasan ICT di Suruhanjaya Koperasi Malaysia yang mana bertujuan untuk menyelaras dan menyeragamkan pengagihan peralatan ICT.

8. PEMAKAIAN DAN TARIKH KUAT KUASA

8.1 Garis panduan ini diguna pakai oleh semua pegawai dan kakitangan di Suruhanjaya Koperasi Malaysia yang berstatus jawatan Tetap, Kontrak, Pekerja Sambilan Harian (PSH), Pegawai Khas, Praktikal / Latihan Industri dan pegawai pinjaman dari luar.

8.2 Garis panduan dikuatkuasakan pemakaiannya pada 15 Oktober 2019.

"BERKHIDMAT UNTUK NEGARA"

(DATUK NORDIN BIN SALLEH)
Pengerusi Eksekutif
Suruhanjaya Koperasi Malaysia

Tarikh : 16/10/2019

NOTA