DASAR KESELAMATAN ICT
VERSI 1.0

SURUHANJAYA PELANTIKAN KEHAKIMAN

JABATAN PERDANA MENTERI

2020

REKOD PINDAAN DOKUMEN

TARIKH	NO. VERSI / PINDAAN	PERKARA	KETERANGAN PINDAAN
15 Jun 2020	1.0	-	Dokumen baru.

KANDUNGAN

MUKA SURAT

B. Pengelasan Dan Pengendalian Maklumat

PERKARA 04 KESELAMATAN SUMBER MANUSIA

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

A. Keselamatan Kawasan

B. Keselamatan Aset ICT

C. Keselamatan Persekitaran

TAFSIRAN

Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan Rahsia Besar.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan Rahsia.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan Sulit.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan Terhad.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Media Storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, kartrij, cakera

	padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta permis berkaitan dengan ICT yang berada di bawah tanggungjawab SPK.
Akaun Pengguna	Akaun e-mel, sistem dan rangkaian.
Kawasan Terperingkat	Kawasan – kawasan premis atau sebahagian dari premis di mana perkara – perkara terperingkat disimpan atau diuruskan atau di mana kerja – kerja terperingkat dijalankan.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada SPK.
Peralatan Perlindungan	Peralatan yang berfungsi untuk pengawalan, pencegahan dan pengurusan tampalan seperti *firewall, router, proxy*, antivirus dan lain-lain.
Enkripsi	Bermaksud menjadikan teks biasa (*plain text*) kepada kod yang tidak dapat difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher* dan bagi mendapatkan semula teks asal tersebut, penyahsulitan digunakan.
Kriptografi	Bermaksud adalah satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
Pengguna	Warga SPK, pembekal, pakar runding dan lain – lain.
Warga SPK	Kakitangan SPK.

PENDAHULUAN

I. PENGENALAN

Dasar Keselamatan ICT SPK mengandungi peraturan-peraturan yang perlu dibaca dan dipatuhi bagi menggunakan aset teknologi maklumat dan komunikasi (ICT) di Bahagian Kabinet, Perlembagaan dan Perhubungan Antara Kerajaan (SPK). Dasar ini juga menerangkan kepada semua pengguna di SPK mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT SPK.

II. OBJEKTIF

Dasar Keselamatan ICT SPK diwujudkan untuk memastikan tahap keselamatan ICT SPK terurus dan dilindungi bagi menjamin kesinambungan urusan SPK dengan meminimumkan kesan insiden keselamatan ICT. Antara objektif keselamatan yang ditekankan di SPK ialah:

a. Kerahsiaan
Data dan maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran.

b. Kawalan Capaian
Kawalan capaian kepada maklumat dan sistem dihadkan kepada pengguna yang layak sahaja.

c. Integriti
Data dan maklumat hendaklah tepat, lengkap dan kemas kini serta ia hanya boleh diubah dengan cara yang dibenarkan sahaja.

d. Keboleh Percayaan Dan Ketersediaan
Maklumat dan sistem operasi fasiliti disediakan apabila pengguna memerlukannya.

III. SKOP

Dasar Keselamatan ICT SPK ini meliputi perlindungan semua bentuk maklumat kerajaan yang dimasuk, diwujud, dimusnah, disimpan, dijana, dicetak, diakses dan diedar. Ini dilakukan melalui pewujudan dan penguatkuasan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a. Perkakasan
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan SPK. Contohnya komputer, pelayan, peralatan komunikasi dan sebagainya;

b. Perisian
Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT;

c. Perkhidmatan
Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contohnya perkhidmatan rangkaian seperti LAN, WAN dan sebagainya, sistem halangan akses seperti sistem kad akses, dan perkhidmatan sokongan seperti kemudahan elektrik, penyaman udara, sistem pencegah kebakaran dan sebagainya;

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

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

f. Premis Komputer Dan Komunikasi
Semua kemudahan serta permis yang digunakan untuk menempatkan perkara (a) hingga (f) di atas.

Dasar ini adalah terpakai kepada semua pengguna di SPK termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT SPK.

IV. PRINSIP - PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT SPK dan perlu dipatuhi adalah seperti berikut:

a. Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "**perlu mengetahui**" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. Hak Akses Minimum

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

c. Akauntabiliti

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

d. Pengasingan

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

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua

rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan(*server*), *router*, *firewall*, IPS, Antivirus dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f. Pematuhan

Dasar Keselamatan ICT SPK hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g. Pemulihan

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

h. Saling Bergantungan

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

V. PENILAIAN RISIKO KESELAMATAN ICT

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

SPK hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/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 SPK 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.

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

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

a. mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b. menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;
c. mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d. memindahkan risiko kepada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

1.1 Pelaksanaan Dasar

Setiausaha SPK adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.

Tanggungjawab: **Setiausaha SPK atau Pegawai yang diturunkan kuasa**

1.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna SPK termasuklah kakitangan, pembekal, pakar runding dan lain-lain yang berurusan dengan SPK.

Tanggungjawab: **ICTSO**

1.3 Penyelenggaran Dasar

Dasar Keselamatan ICT SPK adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan organisasi. Prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT SPK adalah seperti berikut:

1.3.1 mengkaji semula dasar ini sekurang-kurangnya sekali setahun atau mengikut keperluan bagi mengenal pasti dan menentukan perubahan yang diperlukan;

1.3.2 mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Jawatankuasa Pemandu ICT (JPICT) agensi; dan

1.3.3 memaklumkan perubahan yang telah dipersetujui oleh JPICT kepada semua pengguna.

Tanggungjawab: **ICTSO**

1.4 Pengecualian Dasar

Dasar Keselamatan ICT SPK adalah terpakai kepada semua pengguna ICT SPK dan tiada pengecualian diberikan.

Tanggungjawab: **Semua Pengguna SPK**

PERKARA 02 ORGANISASI KESELAMATAN

OBJEKTIF Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.

2.1 Setiausaha SPK

Peranan dan tanggungjawab SU adalah seperti berikut:

2.1.1 memastikan semua pengguna mematuhi Dasar Keselamatan ICT SPK;
2.1.2 memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan
2.1.3 memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT SPK.

Tanggungjawab: **Setiausaha SPK atau Pegawai yang diturunkan kuasa**

2.2 Ketua Pegawai Maklumat (CIO)

Jawatan Ketua Pegawai Maklumat (CIO) adalah jawatan yang disandang oleh Timbalan Setiausaha SPK. Peranan dan tanggungjawab CIO adalah seperti berikut:

2.2.1 membantu SU SPK dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;
2.2.2 menentukan keperluan keselamatan ICT; dan
2.2.3 menyelaras dan menguruskan pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT serta pengurusan risiko dan pengauditan.

Tanggungjawab: **CIO**

2.3 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi SPK ialah Penolong Ketua Setiausaha Penyelidikan (KPSU P), SPK. Peranan dan tanggungjawab ICTSO adalah seperti berikut:

2.3.1 memastikan semua pengguna memahami peruntukan di bawah Dasar Keselamatan ICT SPK;
2.3.2 mengurus program-program keselamatan ICT;
2.3.3 menguat kuasa dan memantau pematuhan ke atas Dasar Keselamatan ICT SPK;
2.3.4 memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT SPK kepada semua pengguna;
2.3.5 mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT SPK;
2.3.6 menjalankan pengurusan risiko;
2.3.7 menjalankan audit, mengkaji semula, merumus tindak balas pengurusan SPK berdasarkan hasil penemuan / keperluan semasa dan menyediakan laporan mengenainya;
2.3.8 memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
2.3.9 melaporkan insiden keselamatan ICT kepada NACSA dan seterusnya memaklumkannya kepada CIO;
2.3.10 mengenal pasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah baik pulih dengan segera;
2.3.11 memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT SPK; dan
2.3.12 membangun, menyelaras dan melaksana pelan latihan dan program kesedaran keselamatan ICT.

Tanggungjawab: **ICTSO**

2.4 Pentadbir Laman Web

Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut:

2.4.1 menerima kandungan laman web yang telah disahkan dan terkini daripada sumber yang sah;
2.4.2 memantau prestasi capaian dan menjalankan penalaan prestasi bagi memastikan akses laman web lancar;

2.4.3 memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai reka bentuk laman web;
2.4.4 menghadkan capaian pentadbir Laman Web ke web *server*;
2.4.5 melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian yang ada pada web *server*;
2.4.6 melaksanakan proses *backup* dan *restore* secara berkala; dan
2.4.7 melaporkan sebarang pelanggaran keselamatan Laman Web kepada ICTSO.

Tanggungjawab: **Pentadbir Laman Web**

2.5 Pentadbir E-Mel

Peranan dan tanggungjawab Pentadbir E-Mel adalah seperti berikut:

2.5.1 menentukan setiap akuan yang diwujud atau dibatal telah mendapat kelulusan terlebih dahulu;
2.5.2 akaun pengguna perlu dibekukan jika pengguna bercuti atau berkursus dalam tempoh panjang atau menghadapi tindakan tatatertib;
2.5.3 mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; dan
2.5.4 memastikan pengguna e-mel berkemahiran mengendalikan e-mel dengan baik.

Tanggungjawab: **Pentadbir E-Mel**

2.6 Pentadbir Rangkaian

Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut:

2.6.1 memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di SPK beroperasi sepanjang masa;
2.6.2 memastikan semua peralatan dan perisaian rangkaian diselenggara;
2.6.3 merancang meningkatkan infrastruktur bagi meningkatkan prestasi rangkaian sedia ada;
2.6.4 mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;
2.6.5 menyediakan zon khas rangkaian bagi tujuan pengujian peralatan dan perisian rangkaian; dan

2.6.6 memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan rangkaian.

Tanggungjawab: **Pentadbir Rangkaian**

2.7 Pentadbir Aplikasi Dan Pangkalan Data

Peranan dan tanggungjawab Pentadbir Aplikasi dan Pangkalan Data adalah seperti berikut:

2.7.1 melaksana pembangunan aplikasi baharu bagi pengurusan maklumat yang sistematik;
2.7.2 melaksana penambahbaikan aplikasi sedia ada bagi meningkatkan kecekapan pengurusan maklumat;
2.7.3 melaksana penyelenggaraan aplikasi dan pangkalan data bagi memastikan ia bersedia untuk digunakan sepanjang masa;
2.7.4 melaksana kerja-kerja *backup* aplikasi dan pangkalan data untuk memastikan keselamatan maklumat terjamin;
2.7.5 memastikan proses *housekeeping* dalam pangkalan data dilaksankan bagi meningkatkan prestasi aplikasi;
2.7.6 memastikan dan melaksanakan prinsip-prinsip DKICT dalam pewujudan akaun pengguna ke atas setiap sistem aplikasi;
2.7.7 memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum aplikasi diaktifkan;
2.7.8 menghadkan capaian dokumentasi sistem aplikasi bagi mengelakkan dari penyalahgunaannya; dan
2.7.9 melaporkan sebarang insiden pelanggaran dasar keselamatan aplikasi dan pangkalan data kepada ICTSO.

Tanggungjawab: **Pentadbir Aplikasi dan Pangkalan Data**

2.8 Pentadbir Keselamatan ICT

Peranan dan tanggungjawab Pentadbir Keselamatan ICT adalah seperti berikut:

2.8.1 memastikan pelaksanaan serta pematuhan dasar, polisi, Prosedur Operasi Kerja (SOP) dan arahan keselamatan ICT SPK dipatuhi;
2.8.2 memastikan laluan trafik keluar dan masuk rangkaian diuruskan secara berpusat dan tidak membenarkan sebarang sambungan ke rangkaian SPK secara tidak sah seperti melalui peralatan modem atau *dail-up*;

2.8.3 melaksanakan penilaian tahap keselamatan sistem rangkaian dan sistem ICT serta penilaian risiko keselamatan maklumat;

2.8.4 memastikan pelaksanaan pelan Pengurusan Kesinambungan Perkhidmatan (PKP) dan data *backup* dapat memastikan keselamatan data terjamin; dan

2.8.5 melaporkan sebarang insiden pelanggaran dasar, polisi, Prosedur Operasi Kerja (SOP) dan arahan keselamatan ICT kepada ICTSO.

Tanggungjawab: **Pentadbir Keselamatan ICT**

2.9 Pengguna

Pengguna adalah warga SPK, pembekal, pakar runding dan pihak-pihak yang terlibat dalam penggunaan dan capaian kepada aset dan perkhidmatan ICT SPK. Peranan dan tanggungjawab pengguna adalah seperti berikut:

2.9.1 membaca, memahami dan mematuhi Dasar Keselamatan ICT SPK;

2.9.2 mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya;

2.9.3 menjalani tapisan keselamatan sekiranya dikehendaki apabila berurusan dengan maklumat rasmi terperingkat;

2.9.4 melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat SPK;

2.9.5 melaksanakan langkah-langkah perlindungan seperti berikut:

i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. memeriksa maklumat dan menentukan ia tepat dan lengkap;

iii. memastikan maklumat sedia untuk digunakan;

iv. menjaga kerahsiaan kata laluan;

v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang berkuat kuasa; dan

vi. melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.

2.9.6 melaporkan sebarang aktiviti yang mengancam keselamatan ICT SPK kepada ICTSO dengan segera;

2.9.7 menghadiri program-program kesedaran mengenai keselamatan ICT;

2.9.8 mengawal aktiviti penggunaan media sosial seperti:

i. mengelakkan ketirisan maklumat;

ii. tidak memberi atau mendedahkan sebarang komen atau penyataan atau isu yang menyentuh perkara-perkara yang boleh menjejaskan imej dan dasar kerajaan;
iii. tidak menyebarkan maklumat yang berbentuk fitnah, hasutan dan lucah atau memprovokasi sesuatu isu yang menyalahi peraturan dan undang-undang atau perkara yang menyentuh sensitiviti individu atau kumpulan tertentu; dan
iv. tidak menggunakan saluran media sosial hingga menggangu fokus dalam urusan kerja.

2.9.9 menandatangani surat akuan pematuhan DKICT SPK seperti Lampiran 1.

Tanggungjawab: **Pengguna**

2.10 Jawatankuasa Pemandu ICT (JPICT) SPK

2.10.1 Keanggotaan JPICT SPK adalah seperti berikut:

Pengerusi : CIO
Ahli :
i. Ketua Penolong Setiausaha
ii. Penolong Pegawai Teknologi Maklumat
iii. Juruteknik Komputer

Urus setia: Unit Teknologi Maklumat

2.10.2 Bidang kuasa JPICT SPK adalah:

i. menetapkan hala tuju dan strategi untuk pelaksanaan ICT di SPK;
ii. merancang, menyelaras dan memantau pelaksanaan projek / program ICT di SPK;
iii. menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik SPK, Pelan Strategik ICT SPK dan Pelan Strategik Teknologi Maklumat Sektor Awam;
iv. memantau perkembanga program ICT serta memahami keperluan, masalah dan isu yang dihadapi dalam pelaksanaan ICT di SPK;

v. memantau dan menentukan langkah-langkah keselamatan ICT; dan
vi. menetapkan dasar dan prosedur pengurusan laman web SPK.

PERKARA 03 PENGURUSAN ASET

A. AKAUNTABILITI ASET ICT

OBJEKTIF **Memberi dan menyokong perlindungan yang optimum ke atas semua aset ICT SPK.**

3.1 Inventori Aset ICT

Memastikan semua aset ICT SPK diberi perlindungan yang bersesuaian oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut:

3.1.1 memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam daftar harta modal dan inventori serta sentiasa di kemaskini;
3.1.2 memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan
3.1.3 mengenal pasti, mendokumenkan dan melaksanakan peraturan bagi penggunaan aset ICT.

Tanggungjawab: **Semua Pengguna SPK**

B. PENGELASAN DAN PENGENDALIAN MAKLUMAT

OBJEKTIF **Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.**

3.2 Pengelasan Maklumat

Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan kepada tahap sensitiviti masing-masing. Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal SPK. Setiap maklumat hendaklah dikelaskan dan dilabelkan

mengikut sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

3.2.1 Rahsia Besar;
3.2.2 Rahsia;
3.2.3 Sulit; atau
3.2.4 Terhad.

Tanggungjawab: **Pegawai Yang Diberi Tanggungjawab**

3.3 Pengendalian Maklumat

Pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut :

3.3.1 menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
3.3.2 memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
3.3.3 menentukan maklumat sedia untuk digunakan;
3.3.4 menjaga kerahsiaan kata laluan;
3.3.5 mematuhi standard, prosedur dan garis panduan keselamatan yang ditetapkan;
3.3.6 memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penyalinan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
3.3.7 menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

Tanggungjawab: **Semua Pengguna SPK**

PERKARA 04 KESELAMATAN SUMBER MANUSIA

OBJEKTIF **Untuk memastikan semua sumber manusia yang terlibat termasuk penjawat awam, pembekal, pakar runding dan pihak-pihak yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT.**

4.1 Sebelum Perkhidmatan

Memastikan penjawat awam, kontraktor, pihak ketiga, pakar runding dan pihak-pihak lain yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan aset ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut:

4.1.1 menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;

4.1.2 menjalankan tapisan keselamatan untuk penjawat awam, pembekal, pakar runding dan pihak-pihak lain yang terlibat selaras dengan keperluan perkhidmatan; dan

4.1.3 mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Tanggungjawab: **Semua Pengguna SPK**

4.2 Dalam Perkhidmatan

Memastikan semua pengguna sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT SPK. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

4.2.1 memastikan semua pengguna SPK mengurus keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh SPK;

4.2.2 memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna

SPK dan sekiranya perlu kepada pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa;

4.2.3 memastikan adanya proses tindakan disiplin ke atas semua pengguna SPK sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh SPK; dan

4.2.4 memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.

Tanggungjawab: **Semua Pengguna SPK**

4.3 Bertukar Atau Tamat Perkhidmatan

Memastikan semua pengguna SPK yang tamat perkhidmatan atau bertukar dari SPK diurus dengan teratur. Perkara yang perlu dipatuhi adalah seperti berikut:

4.3.1 memastikan semua aset ICT Kerajaan dikembalikan kepada SPK mengikut peraturan dan/atau terma yang ditetapkan oleh SPK; dan

4.3.2 membatalkan atau menarik balik kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh SPK.

Tanggungjawab: **Semua Pengguna SPK**

PERKARA 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN

A. KESELAMATAN KAWASAN

OBJEKTIF **Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis dan maklumat.**

5.1 Perimeter Keselamatan Fizikal

Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Perkara yang perlu dipatuhi adalah seperti berikut:

5.1.1 mengenal pasti kawasan keselamatan fizikal dengan jelas dan lokasi serta keteguhan kawasan hendaklah bergantung kepada keperluan untuk melindungi aset dalam kawasan tersebut dan hasil dari penilaian risiko;
5.1.2 memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
5.1.3 memperkukuhkan dinding dan siling;
5.1.4 memasang alat penggera atau kamera litar tertutup (CCTV), jika berkaitan;
5.1.5 menghadkan laluan keluar masuk;
5.1.6 mengadakan kaunter kawalan;
5.1.7 menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan
5.1.8 mewujudkan perkhidmatan kawalan keselamatan.

Tanggungjawab: **CIO dan ICTSO**

5.2 Kawalan Masuk Fizikal

Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis/ bangunan SPK. Perkara yang perlu dipatuhi adalah seperti berikut:

5.2.1 mempamerkan pas keselamatan sepanjang waktu bertugas; dan

5.2.2 mendaftar dan mendapat Pas Keselamatan Pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan bagi setiap pelawat/ pihak luar.

Tanggungjawab: **Semua Pengguna SPK**

B. KESELAMATAN ASET ICT

OBJEKTIF **Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan ke atas aktiviti SPK.**

5.3 Perkakasan

Peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh berfungsi apabila diperlukan. Perkara yang perlu dipatuhi adalah seperti berikut:

5.3.1 memeriksa dan memastikan semua perkakasan ICT di bawah kawalan setiap pengguna berfungsi dengan sempurna;
5.3.2 menyimpan atau meletakkan semua perkakasan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;
5.3.3 menjadi tanggungjawab setiap pengguna di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan
5.3.4 melaporkan sebarang bentuk penyelewengan atau salah guna perkakasan kepada ICTSO / Penyelaras ICT di SPK.

Tanggungjawab: **Semua Pengguna SPK**

5.4 Dokumen

Langkah-langkah pengurusan dokumen yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:

5.4.1 memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
5.4.2 menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit,Terhad dan Terbuka kepada dokumen;

5.4.3 menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan

5.4.4 memastikan dokumen yang mengandungi bahan atau maklumat terperingkat diambil segera dari media *output*.

Tanggungjawab: **Semua Pengguna SPK**

5.5 Media Storan

Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut:

5.5.1 menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;

5.5.2 menghadkan akses untuk memasuki kawasan penyimpanan media kepada pengguna yang dibenarkan sahaja;

5.5.3 merujuk kepada tatacara pelupusan sekiranya penghapusan maklumat hendak dilakukan dan mestilah mendapat kebenaran pemilik maklumat terlebih dahulu; dan

5.5.4 merekodkan pengurusan media termasuk inventori, pergerakan dan penduaan (*backup*).

Tanggungjawab: **Semua Pengguna SPK**

5.6 Media Storan Luaran

Larangan penggunaan media storan luaran seperti disket, pen/*thumbdrive*, *external hard disk*, CD pada rangkaian dalaman (Internal) perlu diberi perhatian, ia bertujuan untuk memastikan tahap keselamatan ICT, SPK adalah sentiasa terpelihara.

5.6.1 hanya media storan yang mendapat pengesahan dan kelulusan penggunaan sahaja yang boleh digunakan pada komputer di SPK. Kebenaran perlu diperoleh dari Unit ICT, SPK; dan

5.6.2 kegagalan mana-mana pegawai atau kakitangan mematuhi arahan tersebut boleh menyebabkan external *devices* yang digunakan dan semua kemudahan ICT pegawai atau kakitangan berkenaan ditarik balik.

Tanggungjawab: **ICTSO**

5.7 Penyelenggaraan Peralatan ICT

Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:

5.7.1 mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggarakan;
5.7.2 memastikan perkakasan hanya diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja;
5.7.3 memeriksa dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan
5.7.4 memaklumkan kepada pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.

Tanggungjawab: **Pentadbir Sistem ICT**

5.8 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat

Peralatan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut:

5.8.1 mendapatkan kelulusan mengikut peraturan di bawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan SPK bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan;
5.8.2 melindungi dan mengawal peralatan sepanjang masa;
5.8.3 memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan; dan
5.8.4 menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.

Tanggungjawab: **Ketua Bahagian / Jabatan**

5.9 Pengendalian Peralatan Luar Yang Dibawa Masuk

Bagi peralatan yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut:

5.9.1 memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT SPK;
5.9.2 mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh SPK bagi membawa masuk / keluar peralatan; dan
5.9.3 memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat kerajaan. Ia perlu disalin dan dihapuskan.

Tanggungjawab: **Semua Pengguna SPK**

5.10 Pelupusan Dan Kitar Semula Peralatan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan SPK:

5.10.1 menghapuskan semua kandungan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran sebelum pelupusan;
5.10.2 merujuk kepada Pekeliling Perbendaharaan Bil. 5 Tahun 2007 "Tatacara Pengurusan Aset Alih Kerajaan"; dan
5.10.3 memastikan setiap peralatan seperti *server*, komputer dan mesin fotostat yang hendak dilupuskan tidak mengandungi data-data terperingkat.

Tanggungjawab: **Semua Pengguna SPK**

5.11 Penggunaan Peralatan ICT Milik Peribadi

Penggunaan peralatan ICT milik peribadi yang bukan dibekalkan oleh SPK untuk urusan kerja rasmi SPK adalah tertakluk kepada perkara berikut:

5.11.1 pengguna mempunyai peranan untuk mengakses dan memproses maklumat;
5.11.2 pengguna perlu mendapatkan kebenaran daripada Pegawai Keselamatan ICT yang bertanggungjawab;
5.11.3 pentadbir Sistem mempunyai hak untuk mengakses, memasang dan memadan perisian kawalan pada peralatan tersebut;
5.11.4 pentadbir Sistem tidak bertanggungjawab ke atas sebarang kehilangan data yang berlaku disebabkan oleh pemasangan perisian kawalan; dan

5.11.5 pemilik peralatan ICT perlu melaporkan kepada Pentadbir Sistem jika peralatan tersebut hilang atau pemilik tidak lagi berkhidmat dengan SPK.

Tanggungjawab: **Semua Pengguna SPK**

C. KESELAMATAN PERSEKITARAN

OBJEKTIF **Melindungi aset ICT SPK daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.**

5.12 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Perkara yang perlu dipatuhi adalah seperti berikut:

5.12.1 merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
5.12.2 melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;
5.12.3 memasang peralatan perlindungan hendaklah di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
5.12.4 menyimpan bahan mudah terbakar hendaklah di luar kawasan kemudahan penyimpanan aset ICT;
5.12.5 meletakkan semua bahan cecair hendaklah di tempat yang bersesuaian dan berjauhan dari aset ICT;
5.12.6 melarang pengguna merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT; dan
5.12.7 memeriksa dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

Tanggungjawab: **Semua Pengguna SPK**

5.13 Bekalan Kuasa

Perkara yang perlu dipatuhi adalah seperti berikut:

5.13.1 menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) atau penjana (*generator*) bagi perkhidmatan kritikal seperti di bilik *server* / pusat data supaya mendapat bekalan kuasa berterusan;
5.13.2 memeriksa dan menguji semua peralatan sokongan bekalan kuasa secara berjadual; dan
5.13.3 melindungi semua peralatan ICT daripada kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai.

Tanggungjawab: **Unit Teknologi Maklumat**

5.14 Prosedur Kecemasan

Perkara yang perlu dipatuhi adalah seperti berikut:

5.14.1 memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan;
5.14.2 melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan Jabatan (PKJ);
5.14.3 mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan
5.14.4 merancang dan mengadakan latihan kebakaran bangunan (*fire drill*) secara berkala.

Tanggungjawab: **Semua Pengguna SPK dan Pegawai Keselamatan Jabatan**

5.15 Kabel

Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Perkara yang perlu dipatuhi adalah seperti berikut:

5.15.1 menggunakan kabel mengikut spesifikasi yang telah ditetapkan;
5.15.2 melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

5.15.3 melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan

5.15.4 melabelkan semua kabel dengan jelas bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.

Tanggungjawab: **ICTSO**

5.16 Clear Desk dan *Clear Screen*

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut:

5.16.1 menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;

5.16.2 menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan

5.16.3 memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.

Tanggungjawab: **Semua Pengguna SPK**

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

A. PENGURUSAN PROSEDUR OPERASI

OBJEKTIF **Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.**

6.1 Pengendalian Prosedur

Memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut:

6.1.1 mendokumenkan semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai, disimpan dan dikawal;

6.1.2 memastikan setiap prosedur mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan

6.1.3 mengemas kini semua prosedur hendaklah dari semasa ke semasa atau mengikut keperluan.

Tanggungjawab: **ICTSO**

6.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut:

6.2.1 memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga;

6.2.2 memantau, menyemak semula dan mengaudit perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga dari semasa ke semasa; dan

6.2.3 mengurus perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur

dan kawalan maklumat sedia ada dengan mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

Tanggungjawab: **ICTSO**

6.3 Perancangan Dan Penerimaan Sistem

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem. Perkara yang perlu dipatuhi adalah seperti berikut:

6.3.1 merancang, mengurus dan mengawal kapasiti sesuatu komponen atau sistem ICT dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang;

6.3.2 memantau dan merancang penggunaan peralatan bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optimum;

6.3.3 menetap kriteria penerimaan untuk sistem maklumat baru, peningkatan dan versi baru dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan

6.3.4 mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

Tanggungjawab: **Pentadbir Aplikasi Dan Pangkalan Data**

6.4 Perlindungan Dari Kod Jahat (*Malicious Code*)

Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *worm*, *trojan* dan *spyware*. Perkara yang perlu dipatuhi adalah seperti berikut:

6.4.1 memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat;

6.4.2 memasang dan menggunakan hanya perisian yang berlesen dan dilindungi di bawah Akta Hak cipta (Pindaan) Tahun 1997;

6.4.3 mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;

6.4.4 mengemas kini *pattern* anti virus dari semasa ke semasa;

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

6.4.6 menghadiri program kesedaran secara berkala mengenai ancaman perisian berbahaya dan cara mengendalikannya;

6.4.7 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;

6.4.8 mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

6.4.9 memberi amaran mengenai ancaman keselamatan ICT dari semasa ke semasa.

Tanggungjawab: **Pentadbir Rangkaian dan Pentadbir Keselamatan ICT**

B. HOUSEKEPPING

OBJEKTIF **Mengekalkan integriti, kebolehsediaan maklumat dan kemudahan pemprosesan maklumat.**

6.5 Penduaan (*Backup*)

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah direkodkan dan disimpan di lokasi yang berlainan. Perkara yang perlu dipatuhi adalah seperti berikut:

6.5.1 membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

6.5.2 membuat salinan penduaan ke atas semua data dan maklumat mengikut kesesuaian operasi;

6.5.3 menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan

6.5.4 membuat dan menguji salinan maklumat dan perisian secara berkala berdasarkan prosedur penduaan.

Tanggungjawab: **Pentadbir Keselamatan ICT**

6.6 Sistem Log

Perkara yang perlu dipatuhi adalah seperti berikut:

6.6.1 mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

6.6.2 menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;

6.6.3 melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan; dan

6.6.4 fail log penggunaan bagi aplikasi yang dianggap kritikal perlu didokumentasikan secara sistematik dan ia boleh dihapuskan jika perlu bagi tujuan penjimatan storan *server*.

Tanggungjawab: **Pentadbir Aplikasi Dan Pangkalan Data**

6.7 Clock Syncronization

Perkara yang perlu dipatuhi adalah seperti berikut:

6.7.1 waktu/masa yang berkaitan dengan sistem pemprosesan maklumat dalam SPK atau *domain* keselamatan perlu diselaraskan dengan satu sumber waktu/masa yang dipersetujui.

Tanggungjawab: **Pentadbir Rangkaian**

C. PENGURUSAN RANGKAIAN

OBJEKTIF **Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal.**

6.8 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti berikut:

6.8.1 membangun dan melaksanakan polisi dan prosedur bagi melindungi maklumat berhubung kait dengan sistem rangkaian;

6.8.2 mengenal pasti ciri-ciri keselamatan, tahap perkhidmatan rangkaian dan memasukkannya ke dalam mana-mana perjanjian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar;

6.8.3 mengasingkan tanggungjawab atau kerja-kerja operasi rangkaian dan komputer untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

6.8.4 meletakkan peralatan rangkaian hendaklah di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan selamat;

6.8.5 mengawal capaian kepada peralatan rangkaian dan terhad kepada pengguna yang dibenarkan sahaja;

6.8.6 memastikan semua peralatan melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

6.8.7 memastikan semua trafik rangkaian melalui *firewall* di bawah kawalan SPK;

6.8.8 melarang semua perisian *sniffer* atau *network analyser* dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

6.8.9 memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”;

6.8.10 Memastikan penggunaan LAN tanpa wayar di SPK mematuhi surat UPTM (S) 159/338/8 Jilid 30 (84) bertajuk “Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless* LAN) di Agensi-agensi Kerajaan”. Polisi penggunaan peralatan *Broadband* Celcom 3G *Wireless*:

i. *Broadband* tersebut hanya akan digunakan apabila rangkaian internet semasa mengalami gangguan;

ii. peralatan tersebut akan diguna pakai untuk Zon Bunga Raya dan juga Zon Melati;dan

iii. bilangan pengguna yang dibenarkan untuk mencapai rangkaian *wireless* bagi setiap unit ialah seramai 5 orang.

Tanggungjawab: **ICTSO**

D. PENGURUSAN MEDIA

OBJEKTIF **Melindungi media ICT daripada kerosakan dan penyalahgunaan.**

6.9 Penghantaran Dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan dan tertakluk kepada prosedur yang sedia ada.

Tanggungjawab: **Pentadbir Keselamatan ICT**

6.10 Pengendalian Media

Prosedur bertujuan mengendali dan menyimpan maklumat daripada didedah tanpa kebenaran atau disalah guna. Perkara yang perlu dipatuhi adalah seperti berikut:

6.10.1 melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
6.10.2 menghadkan dan menentukan capaian mediakepada pengguna yang dibenarkan sahaja;
6.10.3 menghadkan pengedaran media untuk tujuan yang dibenarkan;
6.10.4 merekod dan mengawal aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
6.10.5 menyimpan semua media di tempat yang selamat; dan
6.10.6 menghapus atau memusnahkan media yang mengandungi maklumat rahsia rasmi hendaklah mengikut prosedur keselamatan media yang dikeluarkan oleh kerajaan.

Tanggungjawab: **Pentadbir Keselamatan ICT**

E. KESELAMATAN KOMUNIKASI RANGKAIAN

OBJEKTIF **Memastikan keselamatan pertukaran maklumat dan perisian dalam SPK dan mana-mana agensi luar terjamin.**

6.11 Internet

Prosedur bertujuan mengendali dan menyimpan pertukaran maklumat dengan agensi luar:

6.11.1 laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan;

6.11.2 pihak jabatan berhak menyekat sebarang laman web dan kandungan internet dari semasa ke semasa terutamanya yang berunsur negatif, pornografi, permainan dan perjudian melalui internet;

6.11.3 sebarang penggunaan *Instant Messaging* (IM) dan *web chatting* adalah dilarang kecuali dengan kebenaran pihak pentadbir SPK.

6.11.4 bahan yang diperoleh daripada internet hendaklah ditentukan ketepatan kesahihannya. Sebagai amalan baik, rujukan sumber internet hendaklah dinyatakan;

6.11.5 bahan rasmi hendaklah disemak dan mendapat pengesahan dari Ketua Jabatan sebelum dimuat naik ke internet;

6.11.6 pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak terpelihara;

6.11.7 sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh SPK;

6.11.8 anda dilarang daripada melawat laman-laman pornografi, jenayah dan tidak bermoral yang boleh mencemarkan nama baik anda dan jabatan.

6.11.9 maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk ”Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- agensi Kerajaan” dari semasa ke semasa.

Tanggungjawab: **Semua Pengguna SPK**

6.12 Mel Elektronik

Prosedur bertujuan mengendali dan menyimpan pertukaran maklumat dengan agensi luar:

6.12.1 semua pengguna baru diwajibkan mengisi borang permohonan e- mel sebanyak 2 salinan dan perlu mendapat sokongan dari Ketua Unit masing-masing;

6.12.2 akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh SPK sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

6.12.3 memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

6.12.4 penghantaran e-mel rasmi hendaklah menggunakan akaun e- mel rasmi dan pastikan alamat e-mel penerima adalah betul;

6.12.5 hadkan saiz dan bilangan fail yang ingin anda lampirkan ke dalam e-mel. Semua e-mel (termasuk lampiran) tidak boleh melebihi saiz 10 MB (bersamaan dengan 100 muka surat bersaiz A4), bagi mengelakkan serangan e-mel *bombing* atau penafian perkhidmatan ke atas sistem e-mel jabatan. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

6.12.6 pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

6.12.7 pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

6.12.8 jangan menghantar salinan mesej kepada orang lain yang tidak memerlukannya terutama kepada kumpulan e-mel jabatan (*email groups*). Ini akan membebankan sistem e-mel jabatan terutama sekiranya mesej mempunyai lampiran yang banyak dan bersaiz besar;

6.12.9 e-mel yang tidak penting dan tidak mempunyai nilai arkib, yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

6.12.10 semua e-mel perlu dimuat turun ke *local disk* di PC masing- masing. Emel pengguna hanya disimpan selama 1 tahun di *server* e-mel jabatan, selepas itu e-mel tersebut akan di arkibkan dan mana-mana kekotak e-mel pengguna di *server* yang didapati bersaiz besar melebihi dari 20MB akan dikosongkan tanpa notis;

6.12.11 ketua unit hendaklah memaklumkan kepada pentadbir e-mel menggunakan borang memansuhkan e-mel sekiranya pengguna di bawah jagaannya telah bertukar keluar dari SPK, berpindah agensi, bersara, bercuti panjang, dikenakan tindakan tatatertib, berkursus panjang atau tamat perkhidmatan dan pentadbir sistem perlu membatalkan / membeku / menggantungkan e-mel pengguna tersebut;

6.12.12 akaun e-mel yang didapati tidak digunakan atau tidak aktif lebih daripada 30 hari secara berterusan akan dihapuskan terus daripada sistem e-mel jabatan.

6.12.13 pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat.

6.12.14 penggunaan mel elektronik hendaklah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan pekeliling yang dikeluarkan oleh pihak kerajaan dari semasa-semasa.

6.12.15 polisi penyimpanan e-mel anggota SPK di *server* adalah selama 1 tahun 6 bulan. Selepas tempoh tersebut pentadbir e-mel akan membuat arkib kepada semua e-mel tersebut.

Tanggungjawab: **Semua Pengguna SPK**

6.13 Media Sosial

Prosedur ini bertujuan untuk menerangkan tatacara mengendali kandungan media sosial yang merangkumi laman web SPK, Facebook, Instagram, Twitter, Whatsapp dan sebagainya.

6.13.1 Pengguna SPK dilarang menggunakan media sosial untuk mendedahkan maklumat rasmi yang terkandung dalam dokumen terperingkat Kerajaan kepada pihak umum;

6.13.2 Pengguna SPK dilarang memberikan atau berkongsi komen negative tentang isu-isu yang melibatkan arahan Kerajaan, kepimpinan jabatan dan rakan sekerja; dan

6.13.3 Bagi melancarkan urusan kerja, kumpulan Whatsapp boleh ditubuhkan untuk membincangkan urusan-urusan rasmi pejabat. Hanya kumpulan Whatsapp yang diperakui Setiausaha SPK sahaja dibenarkan untuk perbincangan rasmi.

PERKARA 07 PENGURUSAN INSIDEN KESELAMATAN ICT

OBJEKTIF **Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.**

7.1 Prosedur Pengurusan Insiden

Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut:

7.1.1 mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
7.1.2 menyedia pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;
7.1.3 menyimpan audit trail dan memelihara bahan bukti; dan
7.1.4 menyediakan pelan tindakan pemulihan segera.

Tanggungjawab: **ICTSO**

7.2 Pelaporan Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera. Insiden keselamatan ICT adalah termasuk yang berikut:

7.2.1 maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
7.2.2 sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
7.2.3 kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
7.2.4 berlaku percubaan menceroboh, penyelewengan dan insiden- insiden yang tidak diingini.

Tanggungjawab: **Semua Pengguna SPK**

Nota 2: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.

PERKARA 08 KAWALAN CAPAIAN

OBJEKTIF **Memahami dan mematuhi keperluan keselamatan dalam membuat capaian dan menggunakan aset ICT SPK.**

8.1 Keperluan Dasar

Capaian kepada aset ICT hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, di kemaskini dan dipantau dan menyokong dasar kawalan capaian pengguna sedia ada.

Tanggungjawab: **Semua Pengguna SPK**

8.2 Pengurusan Capaian Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

8.2.1 mewujudkan prosedur pendaftaran dan pembatalan kebenaran kepada pengguna untuk membuat capaian maklumat dan perkhidmatan;

8.2.2 akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat;

8.2.3 akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran Ketua Jabatan secara bertulis dan direkodkan;

8.2.4 pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan Jabatan dan tindakan pengemaskinian dan/atau pembatalan hendaklah diambil atas sebab berikut:

8.2.5 pengguna tidak hadir bertugas tanpa kebenaran melebihi;

8.2.6 satu tempoh yang ditentukan oleh Ketua Jabatan; Pengguna bercuti atau bertugas di luar pejabat dalam satu tempoh yang lama seperti mana yang ditetapkan oleh Ketua Jabatan;

8.2.7 pengguna bertukar jawatan, tanggungjawab dan/atau dikenakan tindakan tatatertib oleh Pihak Berkuasa Tatatertib;

8.2.8 pengguna bertukar, berpindah agensi, bersara dan/atau tamat perkhidmatan.

8.2.9 merekod dan menyenggara aktiviti capaian oleh pengguna dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkodkan termasuk identiti pengguna, sumber yang digunakan,

perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.

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

i. kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun;
ii. kata laluan hendaklah ditukar selepas 90 hari;
iii. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf dan nombor; dan
iv. kata laluan hendaklah berlainan daripada pengenalan Pentadbir Sistem ICT identiti pengguna; dan

Tanggungjawab: **Pentadbir Sistem ICT**

8.3 Tanggungjawab Pengguna

Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:

8.3.1 mematuhi amalan terbaik pemilihan dan penggunaan kata laluan;
8.3.2 memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan
8.3.3 mematuhi amalan *clear desk* / *clear screen policy*.

Tanggungjawab: **Semua Pengguna SPK**

8.4 Kawalan Capaian Rangkaian

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan menempatkan atau memasang antara muka di antara rangkaian SPK dan lain-lain organisasi serta mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut:

8.4.1 memastikan pengguna boleh membuat capaian ke atas perkhidmatan yang dibenarkan sahaja;
8.4.2 mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh;
8.4.3 mengguna kaedah pengenalan automatik berdasarkan lokasi dan peralatan untuk pengesahan sambungan ke dalam rangkaian;
8.4.4 mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;
8.4.5 mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian;
8.4.6 mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan SPK; dan
8.4.7 mewujud dan melaksana kawalan pengalihan laluan (*routing control*) untuk memastikan pematuhan ke atas peraturan SPK.

Tanggungjawab: **Pentadbir Rangkaian**

8.5 Kawalan Capaian Sistem Operasi

Memastikan capaian ke atas sistem operasi dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara berikut:

8.5.1 mengesahkan pengguna yang dibenarkan selaras dengan peraturan SPK;
8.5.2 mewujudkan *audit trail* ke atas semua capaian sistem operasi terutama pengguna bertaraf khas (*super user*);
8.5.3 menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem;
8.5.4 menyedia kaedah sesuai untuk pengesahan capaian (*authentication*); dan
8.5.5 menghadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi adalah seperti berikut:

8.5.6 mengawal capaian ke atas sistem operasi menggunakan prosedur *log-on* yang selamat;

8.5.7 prosedur *log-on* yang selamat perlulah:

i. menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat;

ii. melaksana sistem pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan;

iii. mengawal penggunaan utiliti yang berkeupayaan melepasi sistem dan aplikasi terhad;

iv. menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan

v. menghadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.

Tanggungjawab: **Pentadbir Rangkaian**

8.6 Kawalan Capaian Aplikasi Dan Maklumat

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

8.6.1 membenarkan pengguna membuat capaian aplikasi dan maklumat yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;dan

8.6.2 menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian *malicious* yang berupaya melangkaui kawalan sistem. Perkara yang perlu dipatuhi adalah seperti berikut:

i. membuat capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan, selaras dengan peraturan SPK; dan

ii. mengasingkan persekitaran pengkomputeran yang khusus bagi sistem yang sensitif.

Tanggungjawab: **Pentadbir Aplikasi dan Rangkaian**

8.7 Penggunaan Peralatan ICT Mudah Alih

Memastikankeselamatan maklumat apabila menggunakan kemudahan atau peralatan ICT mudah alih. Perkara yang perlu dipatuhi adalah seperti berikut:

8.7.1 mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan

8.7.2 mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.

Tanggungjawab: **Pentadbir Rangkaian**

PERKARA 09 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

OBJEKTIF Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

9.1 Keperluan Keselamatan

Memastikan kawalan keselamatan yang sesuai dijalinkan ke dalam aplikasi bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut:

9.1.1 menyemak dan mengesahkan data sebelum dimasukkan ke dalam aplikasi bagi menjamin ketepatan maklumat;
9.1.2 menggabungkan semakan pengesahan di dalam aplikasi untuk mengenal pasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan;
9.1.3 mengenal pasti dan melaksana kawalan yang bersesuaian bagi pengesahan dan perlindungan integriti mesej dalam aplikasi; dan
9.1.4 menjalankan proses semak ke atas hasil data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.

Tanggungjawab: **Pentadbir Aplikasi Dan Pangkalan Data**

9.2 Kawalan Kriptografi

Memastikan kaedah kriptografi diguna untuk melindungi kerahsiaan, kesahihan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut:

9.2.1 membangun dan melaksana peraturan untuk melindungi maklumat menggunakan kaedah kriptografi yang sesuai; dan
9.2.2 memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di SPK.

Tanggungjawab: **Pentadbir Aplikasi Dan Pangkalan Data**

9.3 Kawalan Perisian Operasi

Memastikan kaedah yang sesuai dilaksanakan untuk mengawal capaian ke atas fail sistem dan kod sumber program bagi menjamin keselamatan sistem fail. Perkara yang perlu dipatuhi adalah seperti berikut:

9.3.1 mewujudkan peraturan untuk mengawal pemasangan perisian ke dalam persekitaran operasi;
9.3.2 mewujudkan peraturan untuk pemilihan, perlindungan dan kawalan data ujian; dan
9.3.3 mengawal dan menghadkan capaian ke atas kod sumber kepada pengguna yang dibenarkan sahaja.

Tanggungjawab: **Pentadbir Rangkaian**

9.4 Keselamatan Dalam Proses Pembangunan Dan Sokongan

Memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan. Perkara yang perlu dipatuhi adalah seperti berikut:

9.4.1 mengawal pelaksanaan perubahan melalui peraturan formal;
9.4.2 membuat semakan teknikal selepas perubahan sistem operasi bagi menjamin tiada impak negatif ke atas keselamatan operasi SPK;
9.4.3 mengawal dan menghad perubahan ke atas perisian yang perlu sahaja;
9.4.4 menghalang semua peluang untuk kebocoran maklumat; dan
9.4.5 mengawal selia dan memantau pembangunan perisian oleh pihak luar dari semasa ke semasa.

Tanggungjawab: **Pentadbir Keselamatan ICT**

PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

OBJEKTIF Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

10.1 Pelan Kesinambungan Perkhidmatan

Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan SPK dan melindungi aktiviti daripada kesan bencana serta pemulihan perkhidmatan dalam tempoh yang ditetapkan. Perkara yang perlu diberi perhatian adalah seperti berikut:

10.1.1 mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
10.1.2 merancang dan melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
10.1.3. mendokumenkan proses dan prosedur yang telah dipersetujui;
10.1.4 mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan
10.1.5 menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

Tanggungjawab: **ICTSO dan Pentadbir Keselamatan ICT**

PERKARA 11 PEMATUHAN

OBJEKTIF **Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada Dasar Keselamatan ICT SPK.**

11.1 Pematuhan Dasar

Setiap pengguna di SPK hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT SPK, undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

Tanggungjawab: **Semua Pengguna SPK**

11.2 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di SPK:

11.2.1 Keselamatan Perlindungan Secara Am

i. Emergency (Essential Power) Act 1964;
ii. Essential (Key Points) Regulations 1965;
iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982;
iv. Arahan Keselamatan Yang Dikuatkuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985; Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985;
v. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan
vi. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan.

Tanggungjawab: **Semua Pengguna SPK**

11.2.2 Keselamatan Dokumen

i. Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);
ii. Akta Rahsia Rasmi 1972;
iii. Akta Arkib Negara 2003;
iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;
v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (espionage);
vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;
vii. Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui SuraM(R)10308/3/(45) Bertarikh 8 Mei 1987; dan
viii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999.

Tanggungjawab: **Semua Pengguna SPK**

11.2.3 Keselamatan Fizikal Bangunan

i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;
ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;
iii. State Key Points;
iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan;
v. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan Kementerian / Jabatan;
vi. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan

vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.Essential (Key Points) Regulations 1965.

Tanggungjawab: **Semua Pengguna SPK**

11.2.4 Keselamatan Individu

i. Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti;
ii. General Circular Memorandum;
iii. Instruction On Positive Vetting Procedure;
iv. Surat Pekeliling Am Sulit Bil.1/1966 - Perkara Keselamatan Tentang Persidangan- Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;
v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;
vi. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka- mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara tabir Buluh dan Tabir besi;
vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota - Anggota Kerajaan; dan
viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

Tanggungjawab: **Semua Pengguna SPK**

11.2.5 Keselamatan Aset ICT

i. Akta Keterangan 1950;
ii. Akta Tandatangan Digital 1997;
iii. Akta Jenayah Komputer 1997;
iv. Akta Hak Cipta (Pindaan) 1997;
v. Akta Multimedia dan Telekomunikasi 1998;
vi. Surat Pekeliling Am Bil.1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;
vii. Pekeliling Am Bil. 1 Tahun 2001 –Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);

viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi – Agensi Kerajaan;
ix. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;
x. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.
xi. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; dan
xii. Akta dan Peraturan – Peraturan Lain Yang Berkaitan.

Tanggungjawab: **Semua Pengguna SPK**

11.2.6 Keselamatan Penggunaan Media Sosial

i. Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993;
ii. Akta Perlindungan Data Peribadi 2010;
iii. Surat Arahan Ketua Pengarah MAMPU bertarikh 17 Julai 2009 bertajuk “Pelaksanaan Blog bagi Agensi Sektor Awam”;
iv. Surat Arahan Ketua Pengarah MAMPU bertarikh 19 November 2011 bertajuk “Amalan Terbaik Penggunaan Media Jaringan Sosial di Sektor Awam”;
v. Surat Arahan Ketua Pengarah Perkhidmatan Awam bertarikh 7 Jun 2013 bertajuk “Tanggungjawab Pegawai Awam dalam Memelihara Integriti Perkhidmatan Awam Semasa Menggunakan Kemudahan Media Sosial di Internet”;
vi. Surat Arahan Ketua Pengarah Perkhidmatan Awam bertarikh 15 Julai 2016 bertajuk “Larangan Membuat Pernyataan Awam oleh Pegawai Awam”; dan
vii. Garis Panduan Penggunaan E-mel dan Media Sosial SPK Januari 2019.

Tanggungjawab: **Semua Pengguna SPK**

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT SPK

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan – peruntukan yang terkandung di dalam Dasar Keselamatan ICT SPK; dan

2. Jika saya ingkar kepada peruntukan – peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
Jawatan Pegawai Keselamatan ICT
b.p. Setiausaha SPK

Tarikh :