DASAR KESELAMATAN ICT (DKICT)
MAJLIS PERBANDARAN ALOR GAJAH

“ALOR GAJAH BANDAR SEJAHTERA, MAJU DAN DINAMIK”

Diterbitkan Oleh :
Majlis Perbandaran Alor Gajah
Jabatan Teknologi Maklumat
Lebuh AMJ,78000 Alor Gajah,
Melaka

PENGENALAN DOKUMEN

NAMA DOKUMEN : Dasar Keselamatan ICT Negeri Melaka

VERSI : 2.0

TARIKH : 1 JANUARI 2023

I. PENGENALAN

Dokumen Dasar Keselamatan ICT MPAG (DKICT) ini menggariskan **polisi minimum** yang perlu dipatuhi oleh pengurusan dan kakitangan yang berkaitan dengan penggunaan dan pengurusan ICT serta **prosedur umum untuk kegunaan** di Majlis Perbandaran Alor Gajah (MPAG). Walau bagaimanapun, Jabatan/ Unit boleh menggunapakai Dasar Keselamatan ICT atau prosedur masing-masing mengikut kesesuaian

II. PERNYATAAN DASAR KESELAMATAN ICT MPAG

1. Dasar MPAG menetapkan aset ICT dan lain-lain yang berkaitan dengannya mempunyai maklumat kitar hayat yang lengkap bagi membolehkan kakitangan Jabatan dan pihak ketiga melaksanakan tugas dengan telus. Aset-aset tersebut adalah tertakluk kepada kawalan (*control*) yang mencukupi bagi mengelakkan berlakunya kehilangan (*loss*) yang disengajakan atau tidak, akses yang tidak dibenarkan (*unauthorised access*), perubahan yang tidak dibenarkan (*unauthorised manipulation*) atau pendedahan yang tidak dibenarkan (*unauthorised disclosure*).

2. Kawalan yang digunakan mestilah sesuai dengan nilai aset dan pendedahan risiko (*risk exposure*) yang wujud.

3. Dasar ini akan menjadi asas bagi membangunkan polisi dan standard keselamatan ICT yang spesifik untuk menyokong dasar keselamatan ICT Jabatan.

4. Pematuhan kepada DKICT menjamin tahap perlindungan dari berlakunya insiden pencerobohan keselamatan. Ia juga menyediakan respons serta tindakan keselamatan ICT apabila pencerobohan berlaku.

5. DKICT mengesyorkan amalan baik yang berterusan dan perlu dipatuhi (*regimented*).

6. Keselamatan ICT merangkumi perlindungan ke atas semua bentuk maklumat elektronik yang disediakan kepada semua pengguna yang dibenarkan. Ciri-ciri keselamatan maklumat tersebut merangkumi perkara-perkara berikut:

   a) Kerahsiaan – maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

   b) Integriti – data dan maklumat hendaklah tepat, lengkap dan dikemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;

   c) Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d) **Kesahihan –** data dan maklumat hendaklah dijamin kesahihannya; dan

e) **Ketersediaan –** data dan maklumat hendaklah boleh diakses oleh pengguna yang dibenarkan pada bila-bila masa yang diperlukan.

7. DKICT akan mengurangkan ketidaktentuan, persoalan dan ketidakseragaman di dalam mengurus dan menggunakan ICT.

III. OBJEKTIF KESELAMATAN ICT

Objektif keselamatan ICT adalah seperti berikut:

1. Menyediakan prinsip panduan minimum untuk pengurusan yang selamat dan sesuai, penggunaan dan pengoperasian sistem dan aplikasi;

2. Menunjukkan persiapan organisasi yang perlu diwujudkan dari segi fungsi organisasi, kebolehan sumber manusia, kemudahan dan mekanisma untuk operasi dan pengurusan sistem dan aplikasi yang baik;

3. Menyediakan panduan untuk tindakan pembetulan sekiranya berlaku pencerobohan keselamatan atau ketidakpatuhan yang serius;

4. Menerangkan hubung kait antara pihak-pihak yang terlibat dalam khidmat sokongan sistem dan aplikasi, pelaksanaan perubahan terhadap sistem dan aplikasi, dan panduan untuk menerima perubahan yang dibuat ke atas sistem dan aplikasi; dan

5. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

IV. PRINSIP KESELAMATAN ICT MPAG

Dasar Keselamatan ICT MPAG diwujudkan mengikut prinsip-prinsip di bawah:

1. Akses Atas 'Dasar Perlu Mengetahui'

Akses terhadap penggunaan aset ICT hanya dibenarkan 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;

2. Hak Akses Minimum

Tertakluk kepada Para 1, hak akses minimum adalah membaca dan/ atau melihat sahaja. Jika pengguna memerlukan tahap yang lebih tinggi seperti mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat maka kelulusan khas adalah diperlukan;

3. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakan mereka terhadap aset-aset ICT;

4. Pengasingan Kerja

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada penyalahgunaan akses. Pengasingan ini juga termasuk memisahkan kumpulan operasi, pembangunan sistem dan rangkaian;

5. Pengauditan

Pengauditan bertujuan untuk mengenalpasti insiden keselamatan atau keadaan yang mengancam keselamatan. Bagi kelancaran tujuan tersebut aset ICT seperti komputer, pelayan (*server*), *router*, *firewall* dan rangkaian hendaklah menyediakan jejak audit;

6. Pemulihan

Pemulihan sistem amat diperlukan bagi memastikan ketersediaan (*availability*) dan kebolehcapaian (*accessablility*). Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan (*copy*) dan mewujudkan Pelan Pemulihan Bencana ICT (*Disaster Recovery Plan*)/ Kesinambungan Perkhidmatan (*Business Continuity Plan*); dan

7. Pematuhan

DKICT hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk percanggahan yang boleh mendatangkan ancaman kepada keselamatan MPAG.

V. SKOP DASAR KESELAMATAN ICT MPAG

Skop DKICT merangkumi pengurusan, pengendalian dan penyelenggaraan maklumat dan kemudahan ICT termasuk peralatan sokongan**,** borang-borang dan dokumen yang digunakan.

DKICT ini adalah arahan tahap tinggi yang menentukan bagaimana aset ICT diurus, dilindungi dan disebarkan kepada semua Jabatan/ Unit. Pelaksanaan DKICT ini adalah wajib dan setiap Jabatan/ Unit hendaklah mempunyai perancangan untuk menguatkuasa bagi memastikan pematuhan yang menyeluruh.

Semua polisi, arahan, panduan dan prosedur Kerajaan sedia ada hendaklah diutamakan. Walau bagaimanapun, sekiranya terdapat aset yang berklasifikasi tinggi atau operasi yang memerlukan tahap keselamatan lebih tinggi, maka langkah-langkah yang lebih mantap dalam DKICT perlu dipatuhi.

VI. DOKUMEN RUJUKAN

Berikut adalah dokumen-dokumen yang dirujuk semasa penyediaan dokumen ini:

a) MyMIS – Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia;

b) Akta Keselamatan;

c) Akta Rahsia Rasmi 1972;

d) Akta Acara Kewangan 1957;

e) Akta Kawasan Larangan dan Tempat Larangan 1959;

f) Pekeliling Am Bil 3 Tahun 2000 – Rangka Polisi Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

g) Pekeliling Am Bil 1 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

h) Akta Jenayah Komputer 1997;

i) Akta Tandatangan Digital 1997;

j) Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;

k) Arahan Perbendaharaan;

l) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan

m) Dasar Keselamatan ICT (DKICT) Negeri Melaka.

VII. KATEGORI SISTEM DAN APLIKASI DI MPAG

Beberapa aplikasi dan sistem telah dibangunkan dan digunapakai di MPAG. Di samping itu, terdapat juga sistem dan aplikasi yang sedang dalam pembaharuan dan penggantian.

Aplikasi dan sistem (termasuk kemudahan ICT) utama telah dikenalpasti dan dibahagi kepada dua (2) kategori seperti berikut:
i) Kategori 1: Aplikasi penting dan kritikal; dan
ii) Kategori 2: Aplikasi sokongan dan tidak kritikal.

Aplikasi dan sistem Kategori 1 disenaraikan seperti Jadual 1.

Bil.	Sistem atau Aplikasi Penting dan Kritikal	Kegunaan
1.	eKaunter	Sistem kutipan hasil bagi MPAG
2.	FInIS	Mengawal segala bayaran kepada pembekal
3.	Avis	Mengawal proses kutipan cukai
4.	eSewaan	Mengurus dan mengawal proses sewaan gerai
5.	LIMAS	Mengurus dan mengawal proses pelesenan
6.	Kompaun Parking	Mengurus rekod kompaun letak kereta

Jadual 1: Sistem atau Aplikasi Penting dan Kritikal - Kategori 1

VIII. TANGGUNGJAWAB

Semua kakitangan MPAG dan pembekal yang memberi khidmat, atau bertindak selaku ejen kepada Jabatan/ Unit masing-masing hendaklah:

- Mengambil semua langkah untuk menjaga (*safeguard*) maklumat yang wujud, terima atau kawal serta kemudahan yang mereka gunakan;
- Mematuhi Dasar Keselamatan ICT MPAG;
- Melaporkan dengan segera semua insiden keselamatan kepada pihak pengurusan bagi memastikan tindakan yang wajar diambil; dan
- Menggunakan dengan baik aset MPAG dan kemudahan sokongan ICT untuk tujuan yang dibenarkan sahaja.

Penggunaan aset dan kemudahan untuk tujuan selain daripada yang dimaksudkan dan dibenarkan adalah merupakan ketidakpatuhan kepada DKICT yang memungkinkan tindakan disiplin.

IX. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN

Dokumen ini adalah tertakluk kepada kawalan (*subject to document control*) di mana segala perubahan mesti didokumentasikan.

Jabatan Teknologi Maklumat (JTM), Majlis Perbandaran Alor Gajah bertanggungjawab untuk mengemaskini dan memperbetulkan dokumen ini berdasarkan kelulusan Jawatankuasa Pemandu Teknologi Maklumat MPAG.

Jabatan/ Unit lain tidak dibenarkan mengubah dokumen ini. Sebarang permintaan dan cadangan pengubahsuaian atau perubahan hendaklah dihantar kepada JTM di alamat:

Nama	:	Pengarah Jabatan Teknologi Maklumat, Jabatan Teknologi Maklumat
Alamat	:	Aras 2, Blok A, Lebuh AMJ, Alor Gajah, 78000
Melaka		
Telefon	:	+606-556 1000
Faksimili	:	+606-556 4909
E-mel	:	nuridham@mpag.gov.my

X. PENERANGAN TERMINOLOGI FUNGSI

Fungsi/ peranan dan bidang tugas yang terdapat dalam dokumen ini diringkaskan seperti berikut:

Bil.	Nama Peranan	Keterangan Bidang Tugas
1.	Ketua Pegawai Maklumat (CIO)	Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju ICT MPAG.
2.	Pegawai Keselamatan ICT (atau ICTSO Jabatan)	Pegawai Keselamatan ICT Jabatan bertanggungjawab ke atas keseluruhan pematuhan Dasar Keselamatan ICT MPAG. Sekiranya Jabatan memerlukan pengecualian (sementara atau tetap) dalam pematuhan DKICT, maka beliau bertanggungjawab menilai keperluan dan implikasi pengecualian, dan mendokumenkan pengecualian tersebut.
3.	Juru Audit Dalaman	Juru Audit yang dilantik untuk melaksanakan audit dalaman berkaitan pematuhan dasar keselamatan ICT.
4.	Juru Audit Jabatan	Kakitangan Jabatan/ Unit yang ditugaskan untuk menjalankan audit pemantauan dalam Jabatan/ Unit sendiri, dari semasa ke semasa sebagai tugas sampingan.
5.	Juru Audit Luaran	Juru Audit daripada kalangan pakar atau perunding yang boleh melakukan audit teknikal berkaitan pematuhan dasar keselamatan ICT.
6.	Jawatankuasa Pemandu Teknologi Maklumat MPAG	Jawatankuasa ini menentukan hala tuju pelaksanaan ICT MPAG, menetapkan dasar keselamatan ICT dan memantau tahap pelaksanaan serta pematuhan DKICT oleh semua kakitangan MPAG.

Bil.	Nama Peranan	Keterangan Bidang Tugas
7.	Ketua Jabatan/ Unit atau Pegawai Pengawal	Pegawai yang menyokong atau mengesahkan permohonan ID dan hak capaian pengguna dalam Jabatan/ Unit atau kawalannya. Beliau juga bertanggungjawab memaklumkan kepada Pemilik Data atau Pentadbir Keselamatan sekiranya berlaku pertukaran atau persaraan kakitangannya yang mana hak capaian perlu dikemaskini atau dihapuskan.
8.	Khidmat Bantuan Tahap 1	Bantuan dari Jabatan/ Unit sendiri dalam penyelesaian masalah atau insiden dalam Jabatan/ Unit.
9.	Khidmat Bantuan Tahap 2	Bantuan daripada pihak yang membekalkan aplikasi atau sistem dibawah pengurusan Pemilik Aplikasi atau Sistem.
10.	Pemilik Aset	Ketua Jabatan/ Unit yang bertanggungjawab terhadap pemilikan aset bagi pihak Kerajaan.
11.	Pemilik Aplikasi/ Sistem	Pemilik Aplikasi atau Sistem adalah pembekal aplikasi atau sistem tersebut. Pemilik bertanggungjawab atas semua pembetulan fungsi dan naiktaraf aplikasi dan sistem.
12.	Penjaga atau Pengguna Aset	Kakitangan yang bertanggungjawab terhadap ketersediaan aset dan keselamatan aset untuk kegunaan harian.
13.	Pemilik Data	Pemilik Data bertanggungjawab meluluskan permohonan hak capaian yang diperlukan pengguna. **Perhatian:** Sesebuah aplikasi (terutama sekali aplikasi yang besar), boleh ada beberapa Pemilik Data yang berkuasa dan bertanggungjawab ke atas bahagian data bawah tadbiran atau kawalan masing-masing.
14.	Pengguna-Pengguna	Pegawai/ kakitangan yang menggunakan aplikasi atau sistem bagi urusan rasmi.

Bil.	Nama Peranan	Keterangan Bidang Tugas
15.	Pengurus Aplikasi/ Sistem	Pegawai yang bertanggungjawab terhadap aplikasi atau sistem yang dibangunkan dalam Jabatan/ Unit atau dimiliki oleh Jabatan/ Unit. Segala rancangan naiktaraf dan pembetulan diselaraskan oleh Pengurus Aplikasi atau Sistem.
16.	Pentadbir Aplikasi/ Sistem	Pentadbir Aplikasi/ Sistem bertanggungjawab memastikan aplikasi dan sistem berjalan dengan lancar. Antara tugas beliau ialah melaksanakan konfigurasi aplikasi, peruntukkan sumber CPU dan memori (*CPU and memory resources*), melaksanakan '*patches*' dan naiktaraf (*upgrade*), menjana log aktiviti dan membersihkan log.
17.	Pentadbir Pangkalan Data	Pentadbir Pangkalan Data adalah fungsi teknikal yang bertanggungjawab memastikan pangkalan data berfungsi dengan baik dan dikemaskini dari semasa ke semasa. Antara tugas beliau ialah melaksanakan perubahan pangkalan data sekiranya diarahkan oleh pembekal sistem, menjana log, membersihkan log, *re-indexing.*
18.	Pentadbir Keselamatan	Pentadbir Keselamatan bertanggungjawab Melaksanakan permohonan hak capaian pengguna yang telah diluluskan oleh Pemilik Data. Pentadbir Keselamatan boleh mentadbir keselamatan untuk lebih dari satu aplikasi atau sistem.
19.	Pegawai Keselamatan Jabatan (CGSO)	Pegawai yang bertanggungjawab melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

XI. DEFINISI POLISI, STANDARD DAN PROSEDUR

1. Polisi

Polisi adalah kenyataan atau arahan ringkas yang menggambarkan tujuan atau sasaran yang hendak dicapai / menerangkan keperluan setiap domain ICT. Kenyataan polisi adalah ringkas dan padat supaya senang difahami, diingati dan dipatuhi oleh semua yang berkaitan/ terlibat.

2. Standard

Standard menerangkan aktiviti minimum yang mesti dilakukan supaya pelaksanaan nya adalah lebih khusus dan terperinci (*detailed*). Standard boleh dibentuk khusus untuk sesuatu situasi atau keperluan bersesuaian dengan suasana operasi yang disasarkan. Polisi kebiasaannya jarang-jarang bertukar tetapi standard boleh bertukar mengikut perkembangan masa, teknologi, perubahan sistem, suasana atau lokasi kerja, ancaman dan risiko.

3. Garis Panduan

Garis Panduan adalah gabungan cadangan atau '*best practices*' yang digalakkan untuk pematuhan, tetapi tidak diwajibkan. (Garis Panduan tidak disediakan dalam siri dokumen ini sebab ada banyak garis panduan umum berkaitan kegunaan e-mel, perlindungan virus dan lain-lain yang sedia ada.)

4. Prosedur

Prosedur kadangkala dipanggil '*operating procedure*s', '*standard operating procedures*' atau SOP. Prosedur adalah langkah-langkah yang khusus dan tepat bagaimana sesuatu polisi atau standard mesti dilaksanakan. Ini termasuk langkah-langkah yang lebih terperinci (*detailed step*s), borang yang perlu diguna, jadual semakan, aliran proses (*process or workflow*) dan lain-lain. Dalam siri dokumen ini hanya prosedur-prosedur asas sahaja disediakan.

XII. POLISI KESELAMATAN ICT MPAG

Seksyen 1. Polisi Keselamatan Maklumat

1.1. Tujuan dan Skop

Tujuan 'Polisi Keselamatan Maklumat' adalah untuk menyediakan polisi berkaitan keselamatan maklumat yang perlu dipatuhi oleh semua pengguna ICT di setiap Jabatan.

Polisi ini merangkumi seluruh kitar hayat maklumat dan kemudahan pemprosesan maklumat dalam kawalan Jabatan.

1.2. Pernyataan Polisi

Polisi Keselamatan ICT perlu dirangka dan dikemaskini untuk digunapakai dan dipatuhi oleh semua pengguna ICT. Polisi ini perlu disesuaikan mengikut tahap kritikal, risiko sistem dan aplikasi serta proses yang berkaitan dalam Jabatan.

Semua aplikasi dan sistem perlu mematuhi polisi, standard dan prosedur secara minimum. Walau bagaimanapun, bagi aplikasi dan sistem dalam Kategori 1, elemen standard dan prosedur tambahan yang lebih ketat adalah diwajibkan.

Senarai dalam Kategori 1 mesti dikemaskini dari masa ke semasa dengan membuat penilaian terhadap semua aplikasi atau sistem apabila berlaku perubahan skop, proses kerja atau faktor-faktor tertentu yang mungkin mengakibatkan perubahan kategori.

1.3. Prosedur Keselamatan Maklumat

a. Semua kakitangan hendaklah memahami kepentingan aplikasi dan sistem dalam Kategori 1 dan berusaha untuk bekerjasama menguatkuasakan amalan dan prosedur umum yang terkandung dalam dokumen ini dan prosedur khusus yang diwujudkan berasingan;

b. Bukti pematuhan kepada prosedur keselamatan hendaklah disimpan khususnya berkaitan:
   i. Kawalan perubahan dokumen;
   ii. Kawalan rekod aktiviti berkaitan pelaksanaan dan pematuhan prosedur keselamatan;
   iii. Tindakan pencegahan (*preventive action*);
   iv. Tindakan pembetulan (*corrective action*);
   v. Aktiviti audit dan pematuhan; dan
   vi. Rancangan latihan dan pembudayaan keselamatan ICT.
c. Semakan pematuhan dan kemaskini rekod perlu dilakukan sekurang-kurangnya sekali setahun.

Seksyen 2. Pengurusan Keselamatan Maklumat

2.1. Tujuan dan Skop

Tujuan 'Polisi Pengurusan Keselamatan Maklumat' adalah untuk menyediakan satu (1) struktur Pengurusan Keselamatan Maklumat bagi mengurus dan menggunakan sistem dan aplikasi di Jabatan/ Unit mengikut pembahagian tanggungjawab, bidang kuasa dan hubungkait.

2.2. Pernyataan Polisi

Semua kakitangan yang mengguna, mentadbir atau mengurus aplikasi dan sistem di Jabatan/ Unit akan diberi tanggungjawab tertentu seperti yang ditakrifkan di dalam Standard Pengurusan Keselamatan. Kakitangan mesti mematuhi skop tanggungjawab mereka dan melaporkan sebarang pengecualian atau keraguan skop tanggungjawab kepada Ketua Jabatan masing-masing.

2.3. Standard Pengurusan Keselamatan

Maklumat Pengurusan Keselamatan Maklumat dilaksanakan dengan mewujudkan fungsi-fungsi tertentu dengan tanggungjawab tersendiri. Fungsi-fungsi ini perlu bekerjasama dan berhubung kait antara satu sama lain untuk memastikan bahawa keseluruhan objektif keselamatan maklumat tercapai.

Setiap Jabatan/ Unit dikehendaki mematuhi keperluan pengurusan keselamatan maklumat yang praktikal dan bersesuaian dengan kepentingan aplikasi dan sistem yang digunakan. Manakala maklumat milik kerajaan perlu disimpan di premis milik kerajaan dan diuruskan oleh kakitangan kerajaan.

2.4. Jawatankuasa Pemandu Teknologi Maklumat MPAG

a. Dipengerusikan oleh Yang Dipertua MPAG dan dianggotai oleh Ketua Jabatan/ Unit;

b. Menentukan hala tuju pelaksanaan ICT MPAG, menetapkan polisi keselamatan dan memantau tahap pelaksanaan serta pematuhan polisi oleh semua kakitangan MAPG; dan
c. Memberi arahan dari masa ke semasa kepada semua Jabatan/ Unit untuk memantapkan fahaman dan amalan keselamatan maklumat.

2.5. Ketua Pegawai Maklumat

Ketua Pegawai Maklumat (CIO) perlu diwujudkan di setiap Jabatan/ Unit. Peranan dan tanggungjawab CIO adalah seperti berikut:

a. Memastikan Pelan Strategik ICT (PSICT) Jabatan/ Unit selari dengan PSICT Sektor Awam;
b. Melaksana dan Menyelaras Penggunaan Dasar, Standard dan Amalan Terbaik Global;
c. Menyelaras Pembudayaan ICT dalam Sistem Penyampaian Perkhidmatan Jabatan; dan
d. Memantapkan struktur tadbir urus ICT Jabatan/ Unit.

2.6. Pegawai Keselamatan ICT

Pegawai Keselamatan ICT mesti wujud di setiap Jabatan/ Unit. Beliau juga dikenali sebagai ICT Security Officer (ICTSO Jabatan) dan hendaklah memenuhi keperluan kompetensi dan syarat-syarat berikut:

- Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber;
- Memenuhi keperluan pembelajaran berterusan; dan
- Memperolehi tapisan keselamatan daripada jabatan.

Tanggungjawab ICTSO adalah seperti berikut:

a. Merancang, mengurus dan melaksanakan program keselamatan di Jabatan;
b. Memastikan Jabatan/ Unit mematuhi Dasar Keselamatan ICT MPAG;
c. Bekerjasama dengan CGSO MPAG dalam menyelaras dan memberi maklumbalas berkaitan pelaksanaan keselamatan maklumat di Jabatan masing- masing; dan

d. Menilai cadangan atau permohonan pengecualian mematuhi aspek-aspek Dasar Keselamatan, sama ada sementara atau kekal. Beliau hendaklah mengkaji implikasi pengecualian dan mendokumenkan pengecualian tersebut.

2.7. Pegawai Keselamatan Jabatan (CGSO)

Pegawai Keselamatan Jabatan yang dilantik hendaklah terdiri daripada Ketua Jabatan Penguatkuasaan dan Ketua Jabatan Teknologi Maklumat yang bertanggungjawab mengenai pentadbiran Jabatan untuk melaksanakan arahan-arahan keselamatan Kerajaan dengan berhubung rapat dan mendapat nasihat dari Pegawai Keselamatan Kerajaan.

Tanggungjawab CGSO adalah seperti berikut:

a) Bertanggungjawab ke atas semua aspek keselamatan dokumen dan maklumat rasmi Jabatan, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi selaras dengan peraturan- peraturan yang ditetapkan oleh Kerajaan.

b) Mengadakan pemeriksaan dari semasa ke semasa ke atas bangunan, sistem pendawaian elektrik, bilik komputer, bilik dokumen dan peralatan, kawasan pejabat dan semua perkara di bawah tanggungjawabnya bagi mempastikan ia dalam keadaan yang selamat dan tidak terdedah kepada ancaman dan risiko.

c) Menganjurkan kursus dan taklimat kesedaran Keselamatan Perlindungan bagi mempastikan setiap anggota di Jabatan memahami langkah-langkah serta peraturan peraturan Keselamatan Perlindungan.

d) Melaksanakan tugas-tugas lain yang ditetapkan dalam peraturan peraturan keselamatan Kerajaan yang sedang berkuatkuasa dan yang dipinda dari semasa ke semasa.

2.8. Pemilik Aset

Pemilik Aset adalah Ketua Jabatan/ Unit atau Pegawai Pengawal yang bertanggungjawab terhadap pemilikan aset bagi pihak MPAG. Beliau menguruskan rekod dan pelupusan aset.

2.9. Penjaga atau Pengguna Aset

Penjaga atau Pengguna Aset bertanggungjawab terhadap ketersediaan, penyelenggaraan dan keselamatan aset untuk kegunaan harian.

2.10. Pemilik Aplikasi/ Sistem

Pemilik Aplikasi atau Sistem bertanggungjawab terhadap aplikasi atau sistem yang dibekalkan dan sistem yang masih diselenggara oleh pihak ketiga. Segala rancangan naiktaraf dan pembetulan fungsi aplikasi/ sistem diaturkan oleh Pemilik Aplikasi atau Sistem.

Tanggungjawab Pemilik Aplikasi/ Sistem adalah seperti berikut:

a. Membekalkan sistem yang mematuhi aspek-aspek keselamatan mengikut garis panduan Kerajaan dan juga garis panduan dan piawaian yang khusus untuk teknologi yang digunakan;
b. Menyediakan garis panduan yang lengkap berkaitan ciri-ciri keselamatan aplikasi atau sistem dan cara yang efektif untuk menguatkuasakan keselamatan pentadbiran dan kegunaan sistem;
c. Memberi latihan kepada pengguna;
d. Mengkaji maklumbalas dan corak (*trend*) laporan insiden atau masalah berkaitan penggunaan aplikasi dan menyediakan langkah jangka panjang untuk mengelakkan masalah yang sama berulang.

2.11. Pengurus Aplikasi/ Sistem

Pengurus Aplikasi atau Sistem bertanggungjawab menguruskan aplikasi atau sistem yang dibangunkan, dimiliki, ditadbir dan disokong (*support*) sepenuhnya oleh Jabatan/ Unit tersebut. Beliau juga bertanggungjawab terhadap semua rancangan naiktaraf dan pembetulan fungsi aplikasi/ sistem iaitu:

a. Menentukan aplikasi dan sistem mematuhi aspek-aspek keselamatan mengikut garis panduan Kerajaan dan juga garis panduan dan piawaian yang khusus untuk teknologi yang digunakan;
b. Menyediakan garis panduan yang lengkap berkaitan ciri-ciri keselamatan aplikasi atau sistem dan cara yang efektif untuk menguatkuasakan keselamatan dalam pentadbiran dan kegunaan sistem;
c. Memberi dan mengatur latihan kepada pengguna;
d. Mengkaji maklumbalas dan corak (*trend*) laporan insiden atau masalah berkaitan kegunaan aplikasi dan melaksanakan langkah jangka masa panjang untuk mengelakkan berlaku kembali masalah yang sama.

2.12. Pemilik Data

Pemilik Data adalah Pegawai Jabatan/ Unit yang berkepentingan terhadap kerahsiaan dan kesahihan data yang disimpan.

Aplikasi utama boleh mempunyai beberapa Pemilik Data. Mereka mempunyai hak dan tanggungjawab ke atas data tersebut.

a. Bertanggungjawab meluluskan permohonan pengguna untuk hak capaian aplikasi atau modul yang diperlukan;
b. Menentukan hak capaian data mengikut klasifikasi data tersebut;
c. Memantau maklumat yang ditadbir dan mengesan masalah atau kekurangan dari segi kualiti, jumlah atau kewujudan data;
d. Dilarang mengubah data secara terus melainkan menerusi aplikasi; dan
e. Menyemak senarai pengguna dan hak akses pengguna dari semasa ke semasa, dan memberi maklumbalas kepada Pentadbir Keselamatan atau Pentadbir Pangkalan Data berkaitan pengemaskinian senarai hak akses. Ini wajib dilakukan untuk aplikasi Kategori 1, sekurang-kurangnya setahun sekali.

2.13. Pentadbir Aplikasi/ Sistem

Pentadbir Aplikasi/ Sistem hendaklah memmastikan aplikasi berjalan dengan lancar. Di antara tanggungjawab beliau adalah:

a. Melaksanakan konfigurasi aplikasi;
b. Menentukan keperluan sumber *Central Processing Unit* (CPU) dan memori (*CPU and memory resources*);
c. Melaksanakan patches dan naiktaraf (*upgrade*); dan
d. Menjana log aktiviti dan membersihkan log.

2.14. Pentadbir Pangkalan Data

Pentadbir Pangkalan Data bertanggungjawab menentukan pangkalan data berfungsi dengan sempurna dan dikemaskini dari semasa ke semasa. Di antara tugas beliau adalah:

a. Melaksanakan perubahan konfigurasi pangkalan data sekiranya diminta oleh pembekal sistem;
b. Menjana log akses dan perubahan data jika perlu, dan membersihkan log dari semasa ke semasa;
c. Melakukan tuning termasuk *reindexing* apabila diperlukan; dan
d. Memberi hak capaian pangkalan data untuk aplikasi (dan bukan kepada pengguna) dan fungsi bagi backup dan pemulihan (*recovery*).

2.15. Pentadbir Keselamatan

Pentadbir Keselamatan bertanggungjawab melaksanakan permohonan hak capaian pengguna yang telah diluluskan oleh Pemilik Data.

Pentadbir Keselamatan boleh mentadbir keselamatan untuk lebih dari satu (1) aplikasi atau sistem. Di antara tugas beliau adalah:

a. Menyimpan dan menjejak hak capaian (*audit log of access privileges to users*) dan memastikan bahawa kedua-dua rekod tersebut adalah konsisten. Pembetulan perlu dibuat jika terdapat perbezaan;
b. Menyiasat cubaan capaian yang gagal dan mencurigakan (*suspicious failed login attempts*) serta mengambil tindakan sewajarnya, jika perlu; dan

c. Menjana dan menyemak senarai pengguna dan hak akses dari semasa ke semasa serta memajukan senarai tersebut kepada Pemilik Data untuk semakan dan pengesahan. Ini wajib dilakukan untuk aplikasi Kategori 1, sekurang-kurangnya setahun sekali.

2.16. Ketua Jabatan/ Unit atau Pegawai Pengawal

Ketua Jabatan/ Unit atau Pegawai Pengawal bertanggungjawab seperti berikut:

a. Menapis permohonan hak capaian ID dan aplikasi, dan seterusnya menyokong atau mengesahkan permohonan ID dan hak capaian pengguna dalam Jabatan/ Unit atau kakitangan dibawah kawalannya; dan

b. Memaklumkan kepada Pemilik Data atau Pentadbir Keselamatan sekiranya berlaku pertukaran atau persaraan kakitangannya yang mana hak capaian perlu dikemaskini atau dihapuskan.

2.17. Pengguna-Pengguna

Pengguna-pengguna bertanggungjawab seperti berikut:

a. Memahami Dasar Keselamatan ICT dan mempelajari kegunaan sistem atau aplikasi dengan betul dan selamat dan mengamalkannya dengan betul;

b. Mengguna aplikasi atau sistem dalam lingkungan hak capaiannya dan tidak cuba mencerobohi hak capaian yang lain;

c. Menentukan bahawa fail-fail penting yang disimpan dalam komputer kegunaannya disalinkan (*backup*) dari semasa ke semasa;

d. Memaklumkan kepada Pentadbir Keselamatan menerusi Ketua Jabatan/ Unit sekiranya mereka bertukar jawatan dan fungsi supaya hak capaian dapat dikemaskini; dan

e. Melaporkan masalah atau insiden yang berlaku atau disyaki berlaku dengan menggunakan sistem aduan kerosakan sedia ada yang ditadbirkan oleh JTM supaya tindakan dapat diambil untuk diselesaikan.

Seksyen 3. Pengurusan Aset Berkaitan Maklumat

3.1. Tujuan dan Skop

Tujuan Polisi Pengurusan Aset Berkaitan Maklumat adalah untuk merekod semua aset yang berkaitan dengan pentadbiran, pengurusan dan keselamatan ICT, bagi memastikan perlindungan dan kawalan yang sewajarnya dapat dilaksanakan untuk semua proses kerja yang berkaitan. Semua aset yang berkaitan dengan pemprosesan maklumat juga termasuk dalam skop pengurusan aset iaitu:

a. Kakitangan yang mengguna, mentadbir atau mengurus aset berkaitan maklumat; dan
b. Alat sokongan seperti pendingin hawa, *centralised uninterruptible power supply* dan sistem pengesan kebakaran di Pusat Data.

3.2. Pernyataan Polisi

Semua aset perlu dikenalpasti pemilik atau pengurus yang bertanggungjawab terhadap kawalan dan ketersediaannya untuk digunakan atau menyokong proses kerja tersebut. Aset perlu diklasifikasi mengikut kepentingan, diurus dan diselenggara dengan sewajarnya supaya sentiasa berfungsi.

3.3. Standard Pengurusan Aset

Semua aset mesti direkodkan dengan butiran berkaitan seperti:

a. Pemilik Aset (*asset owner*);
b. Penjaga Aset atau Pengguna Aset (*asset custodian*);
c. Klasifikasi aset (untuk aset maklumat atau data);
d. Lokasi aset;
e. Jangkahayat aset (sekiranya maklumat ini ada);
f. Harga perolehan aset (sekiranya maklumat ini ada);
g. Hubung kait aset dengan aset lain (sekiranya maklumat hubung kait aset kurang jelas fungsinya); dan
h. Penyelenggara aset (*asset maintainer*).

Seksyen 4. Keselamatan Sumber Manusia

4.1. Tujuan dan Skop

Tujuan polisi Keselamatan Sumber Manusia adalah untuk mengurangkan risiko kecuaian manusia, kecurian, penipuan atau salahguna kemudahan ICT. 'Polisi Keselamatan Sumber Manusia' perlu dipatuhi oleh semua kakitangan. Manakala prosedur adalah untuk memastikan bahawa sumber manusia diambil kira dalam pelaksanaan Dasar Keselamatan ICT.

4.2. Pernyataan Polisi

Semua kakitangan Jabatan/ Unit hendaklah diberi penerangan mengenai tanggungjawab mereka terhadap penggunaan kemudahan ICT yang betul dan penguatkuasaan Polisi Keselamatan ICT. Semua kakitangan hendaklah mematuhi Prosedur keselamatan yang berkaitan dengan tanggungjawab mereka dan mengamalkan serta menggalakkan penggunaan ICT yang selamat. Kakitangan perlu memberi maklumbalas ke atas sebarang percanggahan di dalam operasi aplikasi atau sistem, keadaan tidak normal atau penyalahgunaan hak. Pihak ketiga/ pembekal juga hendaklah mematuhi Polisi Keselamatan ICT.

4.3. Standard dan Prosedur Keselamatan Sumber Manusia

4.3.1. Tanggungjawab Kakitangan

a. Tanggungjawab dan bidang tugas, termasuk yang berkaitan dengan keselamatan maklumat hendaklah disenaraikan dan diakui oleh kakitangan berkenaan.

b. Kakitangan hendaklah membaca dan memahami bidang tugas, termasuk yang berkaitan dengan keselamatan maklumat seperti terdapat dalam dokumen ini.

4.3.2. Perjawatan Kakitangan

a. Pihak pengurusan hendaklah memastikan bahawa kakitangan yang ditugaskan untuk mengendalikan maklumat

terutama bagi maklumat berperingkat telah menjalani tapisan keselamatan pada tahap yang berpatutan dan bersesuaian dengan peringkat maklumat yang dikendalikan;

b. Prosedur sedia ada dalam penjawatan kakitangan serta tapisan keselamatan hendaklah dipatuhi.

4.3.3. Latihan Kesedaran Keselamatan Maklumat

a. Semua pengguna dan pengendali aplikasi atau sistem perlu diberi latihan atau penerangan berkaitan penggunaan sistem atau aplikasi dan pengendalian maklumat secara betul dan selamat. Mereka juga bertanggungjawab mengesan atau mengenali amalan-amalan yang tidak mematuhi garis panduan kegunaan aplikasi dan sistem secara betul dan selamat oleh pengguna lain; dan
b. Latihan atau penerangan perlu diberikan secara berkala, sekurang-kurangnya setahun sekali. Semua kakitangan hendaklah memperakui kehadiran mereka dalam sesi latihan atau penerangan berkaitan.
c. Jadual latihan hendaklah disediakan setiap tahun oleh JTM dan ICT Jabatan/ Unit dan diaturkan supaya semua kakitangan diberi peluang untuk hadir sekurang-kurangnya sekali setahun.
d. Bahan latihan yang seragam hendaklah disediakan untuk tujuan latihan kesedaran keselamatan maklumat.
e. Latihan ini hendaklah memetik contoh-contoh amalan atau insiden yang pernah berlaku sama ada dalam Jabatan, Kerajaan Negeri atau di luar.
f. Semua pengguna hendaklah menandatangani kehadiran mereka dalam latihan.
g. Meja Khidmat Bantuan hendaklah memberi penerangan ringkas berkaitan Polisi, Standard dan Prosedur kepada pengguna baru sekiranya tarikh latihan yang ditetapkan masih jauh.

4.3.4. Tanggungjawab Kakitangan dan Tindakan Disiplin

a. Semua kakitangan hendaklah dimaklumkan akan tanggungjawab mereka terhadap keselamatan maklumat dan tindakan disiplin yang boleh dikenakan akibat kecuaian dalam mengendalikan maklumat dan mengawal selia keselamatan keadaan sekitar; dan
b. Kakitangan hendaklah menghadiri latihan dan taklimat keselamatan maklumat yang dianjurkan dari semasa ke semasa dan memperakui kefahaman mereka terhadap:
   i. Tanggungjawab dalam memastikan kerahsiaan maklumat;
   ii. Tanggungjawab untuk melaporkan pelanggaran polisi atau ketidakpatuhan terhadap keselamatan pengendalian maklumat atau keselamatan fizikal, walaupun hanya disyaki dan belum terbukti kesilapan tersebut; dan
   iii. Tanggungjawab membantu dan memperingatkan rakan sepejabat serta pelawat-pelawat berkaitan polisi dan standard keselamatan yang perlu dipatuhi.
   iv. Kesedaran dan kefahaman bahawa tindakan disiplin boleh diambil terhadap mereka sekiranya tidak mematuhi polisi keselamatan.

4.3.5. Pengendalian Kakitangan Yang Berpindah Atau Bersara

a. Ketua Jabatan/ Unit hendaklah memaklumkan kepada Pengurus/ Pemilik Aplikasi/ Sistem/ Data sekiranya terdapat kakitangan dibawah jagaannya berpindah atau bersara dan memastikan dikemaskini dalam sistem KMS.
b. Jabatan Teknologi Maklumat perlu mengambil tindakan sewajarnya dalam tempoh 14 hari dari tarikh aduan daripada Jabatan/ Unit.
c. Kata laluan bagi pengguna berkenaan hendaklah diubah selepas tarikh perpindahan atau persaraan kakitangan berkenaan dan Logon IDnya digantung dalam tempoh tiga (3) bulan sebelum dimansuhkan;

d. Ketua Jabatan hendaklah memastikan penyerahan tugas terutama sekali dalam tanggungjawab pengendalian maklumat dilaksanakan kepada pengganti pegawai berkenaan; dan
e. Kakitangan yang bertukar tugas ke Jabatan lain perlu mengisi borang permohonan yang berkaitan sekiranya hendak terus mengguna sistem atau aplikasi yang sama dalam tugas barunya.
f. Prosedur ini tertakluk kepada Sistem/ Aplikasi dan Peralatan ICT di bawah pentadbiran dan seliaan di Jabatan/ Unit masing-masing.

4.3.6. Tindakbalas/ Tindakan Kakitangan Terhadap Insiden Keselamatan

a. Kakitangan yang mengendalikan atau mengguna aplikasi atau sistem diwajibkan melaporkan insiden yang mereka alami atau mereka perhatikan. Laporan perlu disalurkan menerusi Prosedur yang ditetapkan; dan
b. Sekiranya kakitangan mengalami insiden keselamatan sama ada dalam bentuk pencerobohan, gangguan fungsi sistem, serangan virus dan lain-lain hendaklah memantau keadaan dan melaporkan dengan segera dengan menggunakan Sistem KMS di Modul Aduan Aplikasi.
c. Jika laporan dibuat melalui telefon atau e-mel, maka kakitangan tersebut hendaklah menyusulinya dengan Sistem KMS di Modul Aduan Aplikasi yang telah diisi.
d. Kakitangan hendaklah memantau perkembangan penyelesaian insiden atau masalah yang dilaporkan dan berhubung dengan meja Khidmat Bantuan untuk mengetahui tindakan yang akan diambil.
e. Kakitangan hendaklah memberi kerjasama sepenuhnya untuk membantu penyiasatan dan penyelesaian masalah atau insiden yang dihadapi.

f. Kakitangan hendaklah mengesahkan penyelesaian masalah di Sistem KMS di Modul Aduan Aplikasi.

Seksyen 5. Kawalan Fizikal dan Persekitaran

5.1. Tujuan dan Skop

Polisi 'Kawalan Fizikal dan Persekitaran' menetapkan garis panduan bagi tahap minimum perlindungan fizikal untuk kemudahan pemprosesan maklumat dan premis operasi.

Polisi ini berkaitan dengan kemudahan pemprosesan maklumat serta alat sokongan di bawah kawalan setiap Jabatan. Manakala prosedur adalah untuk memberi panduan pengawalan keselamatan fizikal serta penyelenggaraan perkakasan dan persekitaran bagi menyokong keperluan keselamatan ICT.

5.2. Pernyataan Polisi

Kemudahan pemprosesan maklumat hendaklah dilindungi secara fizikal dari ancaman keselamatan dan bahaya persekitaran. Perlindungan untuk kemudahan pemprosesan maklumat adalah perlu bagi mengurangkan risiko akses yang tidak dibenarkan ke atas data dan melindungi dari kehilangan atau kerosakan. Di samping itu, perlindungan juga perlu terhadap kedudukan peralatan, pelupusan, dan juga kemudahan sokongan seperti bekalan elektrik dan infrastruktur pendawaian kuasa dan rangkaian.

5.3. Standard dan Prosedur Kawalan Fizikal Dan Persekitaran

5.3.1. Keperluan Umum

a. Kawasan-kawasan penting atau sensitif perlu dikenalpasti bagi memudahkan kawalan keselamatan dilaksanakan. Kawasan sensitif termasuk pejabat-pejabat penting dan Pusat Data;
b. Semua komputer tidak boleh ditinggalkan dalam keadaan '*logged on*' tanpa kehadiran pengguna; kecuali telah disetkan *screen saver* yang akan berfungsi secara automatik bagi menghalang pengguna lain

menggunakan komputer berkenaan sewaktu ditinggalkan;

c. Semua dokumen dan borang-borang yang digunakan untuk tugas harian hendaklah dikawal daripada berlaku kehilangan, pemusnahan atau kebocoran maklumat kepada pihak yang tidak bertanggungjawab. Penghapusan atau pelupusan dokumen dan borang-borang mesti mengikut garis panduan Kerajaan yang ditetapkan;

c. Semua aset yang telah disenaraikan, terutamanya aset persekitaran dan keselamatan fizikal hendaklah dikenalpasti kedudukan dan kesesuaiannya untuk menyokong operasi;

d. Tempat untuk simpanan rekod-rekod pematuhan keselamatan ICT hendaklah dikenalpasti dan lokasi tersebuthendaklah dikawal;

e. Perkara-perkara yang perlu diberi perhatian atau dipastikan berfungsi adalah seperti berikut:

   i. Sistem kawalan fizikal hendaklah berfungsi dengan sempurna dan senarai kakitangan hendaklah dikemaskini dari semasa ke semasa;

   ii. Buku catitan berasingan hendaklah disediakan untuk merekodkan pergerakan keluar/ masuk pelawat atau pihak penyelenggaraan perkakasan dalam Pusat Data;

   iii. Pendingin hawa yang sesuai dengan kawalan kelembapannya mengikut spesifikasi perkakasan dalam Pusat Data;

   iv. Keupayaan UPS untuk membekalkan kuasa untuk masa yang diperlukan sebelum sistem pelayan dimatikan (*shutdown*) dengan betul;

   v. Keadaan sistem pengesan dan pencegah kebakaran yang sesuai dan berfungsi dengan baik;

vi. Ruang khas yang selamat dan tahan kebakaran disediakan untuk menyimpan *media backup*; dan

vii. Penyelenggaraan berjadual yang perlu dilakukan mengikut panduan pembekal perkakasan. Semua rekod penyelenggaraan hendaklah disimpan dalam tempat selamat.

g. Semua pelawat serta pekerja senggaraan perkakasan diwajibkan memakai pas pelawat. Kakitangan berkaitan hendaklah memastikan mereka dibenarkan ke tempat tertentu sahaja; dan

h. Kerja-kerja penyelenggaraan yang dijalankan oleh pihak ketiga hendaklah disemak oleh kakitangan Jabatan/ Unit yang bertanggungjawab. Semakan dibuat secara *sampling* atau keseluruhan bergantung kepada perkara atau peralatan yang disemak.

5.3.2. Kawalan Keselamatan Fizikal

a. Pintu masuk ke kawasan kritikal atau sensitif hendaklah dilengkapi dengan kawalan kunci elektronik yang boleh merakamkan identiti, tarikh dan masa pergerakan memasuki kawasan itu;

b. Pelawat atau orang luar tidak dibenarkan masuk ke kawasan sensitif atau kritikal tanpa ditemani oleh kakitangan yang dibenarkan. Maklumat keluar masuk pelawat mesti dirakamkan dalam buku catitan pelawat ditempat berkenaan, khususnya di Pusat Data; dan

c. Semua kakitangan dan pelawat dikehendaki mempamerkan pas identiti mereka.

5.3.3. Kawalan Media Storan

a. Pengendalian semua media storan hendaklah dikawal dan dipastikan simpanannya selamat dari ancaman kebakaran atau bencana lain;
b. Pergerakan semua media storan dari suatu tempat ke tempat lain perlu dicatit dan dipantau dari semasa ke semasa; dan
c. Penghapusan media storan hendaklah mengikut garis panduan yang disediakan oleh Kerajaan untuk mengelakkan kebocoran maklumat yang masih ada pada storan tersebut.

Seksyen 6. Pengurusan Operasi dan Rangkaian

6.1. Tujuan dan Skop

Polisi 'Pengurusan Operasi dan Rangkaian' menyediakan garis panduan bagi memastikan prosedur pengurusan operasi dan rangkaian didokumentasi dan dipatuhi. Ini adalah untuk memastikan kesediaan operasi dan rangkaian bagi menyokong proses kerja.

Polisi ini berkaitan dengan semua kemudahan pemprosesan maklumat dan alat sokongan di bawah kawalan setiap Jabatan. Manakala prosedur adalah untuk menentukan bahawa amalan operasi, kendalian, perubahan dan pembaikan sistem dilaksanakan dengan teratur dengan menggunakan borang-borang yang berkaitan.

6.2. Pernyataan Polisi

Pentadbir Sistem hendaklah memastikan pengurusan dan pengoperasian yang baik ke atas semua kemudahan pemprosesan maklumat dan mengurangkan gangguan sistem. Amalan pengurusan operasi dan rangkaian hendaklah memastikan matlamat kerahsiaan, integriti, dan ketersediaan tercapai. Ini termasuklah pengasingan tugas, daftar aktiviti (*loggin*g) serta menyemak aktiviti penting, memastikan prosedur *backup* dijalankan dan baikpulih dapat dilaksanakan sekiranya berlaku gangguan.

Perubahan ke atas sistem (*patches)* hendaklah dilakukan secara terkawal dan berdasarkan keperluan Jabatan. Perancangan dan perlaksanaan hendaklah diluluskan oleh pihak pengurusan selepas memastikan keserasian kesemua komponen dikekalkan.

6.3. Standard dan Prosedur Pengurusan Operasi dan Rangkaian

6.3.1. Pengurusan Konfigurasi

6.3.1.1. Pengurusan Konfigurasi Sistem

a. Semua perkakasan ICT, perisian dan peralatan sokongan perlu:

i. Direkod semasa penyerahan dari pembekal alat dan/atau sistem untuk kegunaan;

ii. Dikemaskinikan rekodnya apabila berlaku perubahan, penukaran atau naiktaraf; dan

iii. Diselaraskan rekod asetnya yang berkaitan sebagaimana disebutkan dalam seksyen 3.3.

b. Perubahan kepada aset atau konfigurasi aset termasuk perisian hanya boleh dibenarkan selepas mendapat kelulusan Pemilik Aset atau pihak pengurusan. Pemilik Aset atau pihak pengurusan akan mempertimbangkan permohonan atau cadangan perubahan konfigurasi selepas mengambilkira:

i. Asas keperluan perubahan;

ii. Peruntukan sumber (*resource allocation*) pada pelayan;

iii. Cara perubahan akan dilaksanakan termasuk:

- Jadual perlaksanaan perubahan; dan
- Senarai ujian penerimaan (*list of tests for acceptance of change and acceptance criteria*).

iv. Tatacara kembali kepada konfigurasi asal sekiranya berlaku masalah semasa perubahan atau setelah perubahan dilakukan (*back-out or undo procedure*);

v. Pelan pemantauan sistem selepas perubahan dilakukan (system monitoring plan and monitoring timeframe after changes are made);

vi. Implikasi dan program perubahan tatakerja termasuk latihan, sekiranya perubahan

memerlukan atau mengakibatkan perubahan proses kerja atau prosedur (*work change management*); dan

vii. Rancangan Pengurusan Perubahan (*Change Management Plan*) kepada yang berkaitan.

6.3.1.2. Pengurusan Konfigurasi Perkakasan

a. Konfigurasi perkakasan, perisian dan rangkaian hendaklah dicatit atau dicetak dan disimpan sebagai *snapshot* untuk rujukan;
b. Sekiranya insiden atau masalah berlaku, *snapshot* konfigurasi ini hendaklah dibandingkan dengan konfigurasi sebenar dengan menggunakan perisian pemantauan atau yang setara; dan
c. Cetakan konfigurasi hendaklah disimpan ditempat selamat.

6.3.1.3. Pengurusan Konfigurasi Teknikal

a. Konfigurasi teknikal teknikal merupakan konfigurasi asas bagi perkakasan dan sistem.
b. Sekiranya perubahan konfigurasi perkakasan tersebut perlu dilakukan dengan menggunakan ID Pentadbir, maka hendaklah direkodkan.
c. Laporan perubahan yang dilakukan hendaklah dicetak dan dibandingkan tempoh kegunaannya.
d. Rekod-rekod perubahan konfigurasi (sebelum dan selepas perubahan) hendaklah disimpan ditempat yang selamat.

6.3.1.4. Pengurusan Konfigurasi Rangkaian

a. Pengurusan konfigurasi rangkaian perlu dijalankan untuk memantapkan prestasi rangkaian dan keselamatan sistem. Pengurusan konfigurasi peralatan rangkaian adalah seperti berikut:

i. Polisi peralatan rangkaian seperti Firewall, Web Filter dan Web Application Firewall, Mail Filter, Load Balancer dan Antivirus;
ii. Alamat IP rangkaian untuk setiap segmen sedia ada seperti LAN, DMZ dan WAN sama ada secara DHCP atau statik;
iii. Rangkaian wireless atau bridging; dan
iv. Rangkaian LAN seperti switch atau hub.

b. Kakitangan terlatih dan berpengalaman diperlukan bagi merancang dan melaksanakan perubahan konfigurasi tersebut dan perlu memahami perkara-perkara berikut:
   i. Keperluan perubahan konfigurasi;
   ii. Implikasi perubahan konfigurasi; dan
   iii. Tatacara menyelesaikan masalah konfigurasi
c. Rekod perubahan konfigurasi (sebelum dan selepas perubahan) hendaklah diarkibkan;
d. Sebarang permohonan perubahan polisi hendaklah dimohon oleh Pentadbir Sistem sendiri kepada Penjaga Aset;
e. Semua perubahan besar hendaklah mendapat kelulusan pemilik, manakala perubahan biasa hanya perlu mendapat kelulusan Penjaga Aset; dan
f. Rekod perubahan konfigurasi hendaklah disimpan;
g. Bagi **perubahan sistem yang melibatkan aplikasi dan sistem dalam Kategori 1**;
   i. Keperluan memaklumkan dan mendapat kelulusan seperti di perenggan 6.3.1.1-b wajib dipatuhi; dan
   ii. Semua aktiviti perubahan perlu dicatitkan oleh pelaksana perubahan untuk disemak oleh Penjaga Aset selepas perubahan dilaksanakan.

6.3.1.5. Perubahan Konfigurasi Sementara

a. Semua permintaan perubahan konfigurasi sementara hendaklah disalurkan kepada Penjaga Aset untuk pertimbangan dan kelulusan. Diantara tujuan perubahan konfigurasi adalah seperti berikut:

   i. Pembukaan *port* tertentu pada *firewall* untuk penyiasatan masalah; dan

   ii. Perubahan rangkaian untuk ujian.

   Maklumat yang perlu dikemukakan untuk pertimbangan

   termasuk:

   i. Tujuan keperluan perubahan;

   ii. Tempoh perubahan; dan

   iii. Risiko perubahan dan cara mengatasi atau mengawalnya.

b. Permohonan **perubahan sementara boleh dibuat atas keperluan** penyelesaian insiden atau masalah yang dilaporkan melalui Sistem KMS di Modul Aduan Aplikasi;

d. Penjaga Aset hendaklah menentukan bahawa semua perubahan sementara dilaksanakan dalam tempoh yang diluluskan dan semua konfigurasi diubah ke konfigurasi asal sebelum tamat tempoh melainkan konfigurasi sementara tersebut diperlukan sebagai penyelesaian tetap; dan

e. **Untuk perubahan sementara yang melibatkan sistem atau aplikasi dalam Kategori 1**;

   i. Semua aktiviti kerja perubahan hendaklah dicatitkan oleh pelaksana perubahan dan log perubahan perlu dijana untuk disemak oleh Penjaga Aset selepas kerja-kerja perubahan dilaksanakan/ dijalankan; dan

ii. Pemilik Data aplikasi atau sistem yang terlibat perlu dimaklumkan berkaitan kerja-kerja perubahan sementara tersebut.

6.3.1.6. Perubahan Konfigurasi Dalam Keadaan Kecemasan

a. Perubahan konfigurasi dalam keadaan kecemasan (*Emergency Configuration Changes*) hanya boleh dilakukan apabila sistem memerlukan tindakan perubahan serta merta untuk meneruskan perkhidmatan atau melaksanakan urusan penting;

b. Permohonan perubahan kecemasan juga boleh dilakukan atas keperluan penyelesaian insiden atau masalah yang dilaporkan;

c. Perubahan dalam keadaan kecemasan boleh dilakukan oleh Penjaga Aset*;* Penjaga Aset boleh menjalankan kerja perubahan kecemasan apabila beliau telah menentukan bahawa itulah yang sepatutnya dilakukan untuk menyelesaikan masalah;

d. Untuk aplikasi atau sistem dalam Kategori 1, Pemilik Aset hendaklah menentukan bahawa perubahan konfigurasi serta merta memang perlu (dan tidak ada jalan lain atau tidak boleh ditangguhkan) dan meluluskannya sebelum perubahan dijalankan oleh Penjaga Aset, terutama sekali perubahan yang kritikal atau sensitif;

Untuk aplikasi atau sistem dalam Kategori 1, semua perubahan konfigurasi hendaklah direkodkan selepas pelaksanaan (*retrospectively*) dan semua jejak audit perlu disimpan untuk semakan;

g. Pemilik Aset hendaklah memantau kekerapan perubahan dalam keadaan kecemasan dan

merangka tindakan jangka panjang untuk mengurangkan perubahan:

i. memantau dan menyemak kekerapan perubahan dalam keadaan kecemasan; dan

ii. merangka tindakan jangkamasa panjang untuk mengurangkan perubahan yang dilakukan secara kecemasan. Pemantauan atau semakan boleh dilaksanakan mengikut prosedur seperti Seksyen 9.

6.3.2. Pengasingan Kerja

a. Pengasingan kerja mesti dilaksanakan untuk aplikasi atau sistem dalam Kategori 1. Untuk lain-lain aplikasi atau sistem yang bukan dalam Kategori 1, sekiranya pengasingan kerja tidak dapat dilaksanakan atas sebab-sebab tertentu, maka Logon ID yang berasingan perlu diwujudkan dan digunakan untuk tugas-tugas yang memerlukan pengasingan kerja (walaupun digunakan oleh seorang individu sahaja) Ini adalah untuk memudahkan pemantauan kegunaan ID, sesuai dengan kerja-kerja yang dijalankan; dan

b. Pastikan bahawa semua aktiviti penting yang menggunakan ID berkenaan hendaklah mempunyai *audit trail*, dan **ini diwajibkan untuk aplikasi atau sistem dalam Kategori 1**.

6.3.3. Kawalan Kegunaan ID Hak Capaian Tinggi

a. ID Pentadbir Sistem (Administration ID), Root atau Super user wujud untuk setiap sistem seperti pelayan, OS, pangkalan data, alat rangkaian dan firewall. Kegunaan ID yang mempunyai hak capaian paling tinggi (access privileges) perlu dikawal kegunaannya;

b. Untuk aplikasi atau sistem dalam Kategori 1, ID Hak Capaian Tinggi hendaklah digunakan untuk mewujudkan

ID khusus dan terhad (*limited*). ID tersebut digunakan untuk tujuan yang telah ditetapkan seperti melakukan backup, mengaktifkan perkhidmatan (*services*) yang diperlukan, mengubah konfigurasi dan memantau kegunaan sistem (*system resource monitoring and network utilisation monitoring*);

c. ID khusus dan terhad hendaklah digunakan untuk tadbiran harian, manakala ID yang tinggi hak capaiannya tidak harus digunakan untuk tugas pemantauan dan senggaraan harian.

d. Sekiranya ID yang tinggi hak capaiannya perlu digunakan, maka pastikan bahawa semua permohonan dan gerak langkah penggunaan dipantau.

e. Pentadbir Aplikasi/ Sistem, Pentadbir Pangkalan Data, Pentadbir Keselamatan serta pentadbir-pentadbir lain yang perlu mengguna ID hak capaian tinggi hendaklah memberi sebab yang kukuh sebelum diluluskan oleh Pegawai Keselamatan ICT Jabatan/ Unit.

g. Semua rekod kegunaan ID yang tinggi hak capaiannya hendaklah dicatitkan untuk semakan dari semasa ke semasa dan disimpan dalam simpanan rekod.

6.3.4. Prosedur Operasi (Operating Procedures) dan Dokumentasi

a. Semua prosedur penting berkaitan pengendalian aplikasi dan sistem hendaklah didokumen dan dikemas kini dari masa ke semasa dan pastikan dokumentasi tersebut mempunyai kawalan perubahan dokumentasi. Prosedur-prosedur ini termasuk;

   i. Memula dan menamatkan sistem (*start up and shutdown*);

   ii. Kawalan perubahan aplikasi atau sistem (*configuration change control*);

   iii. Backup and recovery;

iv. Tatacara menganalisa dan mengesan masalah (*troubleshooting and problem tracing*);
v. Selenggaraan sistem (*maintenance and housekeeping*);
vi. Kawalan keselamatan (*security and control*); dan
vii. Rekod-rekod yang perlu didokumenkan.

b. Pembahagian tanggungjawab dan antaramuka (*interface*) semua yang terlibat mentadbir dan melaksanakan prosedur berkaitan perlu disenaraikan bersama dalam dokumen prosedur;
c. Dokumentasi berkaitan perlu disebarkan kepada semua yang berkenaan dengan arahan untuk melupuskan muka surat dokumentasi yang lama yang telah diganti atau dibatalkan; dan
d. Senarai penerima dokumentasi disediakan supaya pembahagian dokumentasi tepat dan terkawal.

6.3.5. Penyelenggaraan Aplikasi atau Sistem

a. Pastikan Pembekal dan Pemilik Aplikasi/ Sistem memantau penyelenggaraan aplikasi dan sistem berkaitan dari semasa ke semasa supaya penggunaan aplikasi atau sistem tidak terganggu dan berjalan lancar. Ini termasuk:
   i. '*Pangkalan Data recovery logs'*, dan lain-lain fail yang perlu dibersihkan dari masa ke semasa;
   ii. Penyusunan dan pengindeksan semula pangkalan data (bergantung kepada jenis teknologi pangkalan data yang digunakan dan rekabentuk sistem); dan
   iii. Pengosongan fail-fail sampingan yang mengandungi *audit trail.*
b. Pastikan semua fail disalinkan ke media bersesuaian sekiranya perlu sebelum mengosongkannya;
c. Langkah terperinci untuk penyelenggaraan setiap komponen sistem hendaklah didokumenkan mengikut kawalan dokumen;

d. Satu jadual penyelenggaraan sistem perlu disediakan untuk semua perkakasan dengan butiran yang perlu diselenggarakan pada tahap jadual tertentu. Satu jadual perlu disediakan oleh penyelenggara (pihak ketiga) untuk kelulusan bahagian ICT Jabatan/ Unit;
e. Sekiranya jadual penyelenggaraan perlu ditangguhkan, maka aktiviti tersebut hendaklah dilakukan secepat mungkin selepas penangguhan;
f. Perkakasan yang diganti atau dibaiki hendaklah dicatitkan dan rekod konfigurasi hendaklah dikemaskini sekiranya berlaku perubahan perkakasan atau komponen; dan
g. Untuk penyelenggaraan yang dilakukan oleh pihak ketiga, pastikan penggunaan ID aplikasi atau sistem yang terhad untuk kegunaan mereka.

6.3.6. Perjanjian Tahap Perkhidmatan(SLA)

a. Pastikan bahawa wujudnya Perjanjian Tahap Perkhidmatan terutama sekali dengan pembekal perkhidmatan luar atau penyelenggara aplikasi dan sistem dan alat sokongan yang sesuai dan tepat dengan kepentingan perkhidmatan yang disasarkan. Perjanjian tersebut sekurang-kurangnya hendaklah mengandungi:
    i. Senarai jenis gangguan atau masalah dan tempoh baikpulih;
    ii. Tanggungjawab pihak yang berkaitan dalam menyelenggara, melapor, menyiasat dan membaikpulih gangguan;
    iii. Nombor telefon dan faks pembekal perkhidmatan;
    iv. Pengecualian, jika ada;
    v. Penamatan; dan
    vi. Penalti atau pemulangan pembayaran (*rebate*) sekiranya pembekal perkhidmatan tidak dapat memenuhi perjanjian tersebut.

b. Tentukan bahawa peruntukan SLA memenuhi keperluan keselamatan sistem;

c. Pastikan semua maklumat dicatit jika pembekal pekhidmatan luar dipanggil untuk menyelesaikan gangguan;

d. Adakan mesyuarat untuk membincangkan jenis gangguan dan pematuhan SLA dan rancang masa depan untuk mengurangkan gangguan dari semasa ke semasa; dan

e. Pastikan semua bukti dan butiran sedia ada untuk membuat tuntutan (sekiranya ada).

6.3.7. Backup dan Media Backup

a. Semua media *backup* hendaklah digunakan mengikut panduan kegunaan dan bilangan kegunaan semula (*maximum number of times reusable or recycle*) dan tempoh kegunaan (*shelf life*) dari pembekal;

b. Media *backup* diuji dari semasa ke semasa untuk memastikan ia berfungsi dengan baik;

c. Rekod bagi jejak dan kitaran setiap media hendaklah disimpan;

d. Media *backup* perlu disimpan di bangunan berasingan yang sesuai dan selamat. Pastikan media dapat digunakan semasa pemulihan aplikasi atau sistem;

e. *Backup* perlu dilakukan mengikut Prosedur MS ISO 9001:2015

f. Adakan jadual backup yang bersesuaian dengan kegunaan aplikasi;

g. Kekerapan aktiviti *backup* berdasarkan Prosedur MS ISO 9001:2015

h. Pastikan bahawa fail penting tidak disimpan dalam PC atau *notebook*. Ruang bagi pengguna hendaklah disediakan dalam *cloud* supaya *backup* berjadual boleh dilakukan; dan

i. Pengguna hendaklah melakukan *backup* sendiri bagi fail-fail penting dan menyimpannya ditempat yang selamat.

j. Bekas media sandaran, lokasi dan infrastruktur yang menempatkan bekas media sandaran hendaklah disahkan oleh petugas di lokasi tersebut.

6.3.8. Komputer MPAG

a. Komputer yang dipasang di Pejabat Cawangan dan Jabatan-jabatan disambung kepada rangkaian yang ditadbirkan oleh JTM. Perubahan atau tambahan sambungan ke rangkaian lain dilarang dilakukan oleh pengguna melainkan atas kebenaran kakitangan selenggaraan JTM.

b. Pihak JTM bertanggungjawab menguruskan pemasangan komputer di Jabatan/ Pejabat Cawangan termasuk sambungan ke rangkaian VPN.

c. Pengguna tidak dibenarkan mengubah pemasangan komputer atau menyambung komputer ke rangkaian lain (contoh: menerusi dial-up, 'wireless LAN', 3G kecuali Bluetooth) tanpa kebenaran pihak JTM.

d. Pengguna dikehendaki bekerjasama membuat ujian atau mengubah sementara sambungan ke rangkaian atas arahan kakitangan penyelenggaraan JTM semasa penyiasatan penyelesaian masalah secara jarak jauh (*remote*).

6.3.9. Rangkaian Tanpa Wayar

a. Rangkaian tanpa wayar (Open Wireless) yang disediakan di MPAG adalah untuk kegunaan orang awam dan pelawat yang datang berurusan.

b. Pengguna yang ingin memasang atau mengguna rangkaian tanpa wayar (wireless network) hendaklah memahami risiko dan keupayaan mereka untuk mengendalikan perkakasan tersebut.

d. Pegawai Keselamatan ICT MPAG hendaklah mengkaji permohonan keperluan, suasana kegunaan, lokasi perkakasan, penyelenggaraan, konfigurasi IP dan cara kegunaan yang dicadangkan oleh pemohon dan menggariskan syarat-syarat yang perlu dipatuhi.

e. Pemohon hendaklah mengesahkan syarat-syarat yang digariskan sebelum kelulusan diperolehi.

f. Kelulusan hanya diberi untuk satu tempoh masa yang dinyatakan dalam syarat-syarat tersebut dan permohonan semula perlu dibuat sekiranya penggunaan diperlukan selepas tempoh tersebut.

6.3.10. Perancangan Kapasiti Perkakasan

a. Penggunaan aplikasi atau sistem hendaklah dipantau dari semasa ke semasa. Kajian perancangan perlu dilakukan setiap tahun bagi memastikan tahap perkhidmatan yang disasarkan tercapai. Perkara-perkara yang perlu dilakukan adalah:

   i. Menentukan keupayaan perkakasan seperti CPU, *Random Access Memory* (RAM), perkakasan rangkaian dan keselamatan (switches, IDS dan firewall); dan

   ii. Memastikan kapasiti storan mencukupi melalui penggunaan suatu sistem pemantauan perkakasan dan rangkaian serta hasil penyelenggaraan berkala peralatan di MPAG.

b. Bahagian ICT MPAG hendaklah memantau semua sumber secara berkala atau sekurang-kurangnya sekali setahun bagi menentukan keupayaan perkakasan sedia ada melalui penggunaan suatu sistem pemantauan perkakasan dan rangkaian serta hasil penyelenggaraan berkala peralatan ICT di MPAG.

c. Di antara perkakasan yang perlu dipantau adalah seperti berikut:

i) *CPU, RAM, Switches, IDS & Firewall*:

- Pastikan berfungsi dengan sempurna.

ii) Aplikasi dan Sistem:

- Masa respon mengikut piawaian yang telah ditetapkan.

iii) Cakera keras:

- Kapasiti storan yang mencukupi.

d. Peningkatan dan penambahbaikan perkakasan hendaklah dirancang dan diperolehi untuk mencapai tahap perkhidmatan yang disasarkan.

e. Pengumpulan data hendaklah mengambil kira semua penggunaan sistem yang tinggi dan sederhana serta mengkaji tahap peningkatan yang sesuai dengan keperluan dan kos.

f. Bajet dan jangka masa hendaklah diambilkira semasa membuat perancangan naik taraf atau gantian sistem.

g. Kos naik taraf hendaklah dibandingkan dengan kos gantian serta tempoh sokongan (*support*) perkakasan oleh pembekal sebelum sesuatu keputusan dibuat.

6.3.11. Penggunaan Perisian Anti-Virus

a. JTM hendaklah menetapkan perisian *anti-virus* untuk diselaraskan dalam Jabatan/ Uniti.

b. Komputer MPAG hendaklah ditetapkan konfigurasinya untuk mengemaskini perisian *anti-virus* dan secara automatik.

6.3.12. Simpanan Rekod dan Pengurusan Kualiti

a. Semua rekod penting berkaitan konfigurasi asal dan perubahan- perubahan yang dilakukan kepada aplikasi atau sistem atau peralatan rangkaian dan peralatan keselamatan hendaklah disimpan; dan

b. Untuk aplikasi dan sistem dalam Kategori 1, kajian perlu dilakukan setiap tahun untuk membandingkan konfigurasi sedia ada dengan catatan-catatan rekod

perubahan bagi mempastikan konsistensinya. Jika terdapat perbezaan, perlu dibetulkan atau diselaraskan.

c. Semua rekod penting berkaitan konfigurasi asal dan perubahan yang dilakukan kepada aplikasi atau sistem atau perkakasan rangkaian dan keselamatan hendaklah disimpan dalam ruang simpanan rekod.

d. Semua rekod hendaklah ditanda dan disenaraikan bagi memudahkan jadual pengemaskinian rekod lama dilakukan.

e. Sistem penyenaraian hendaklah mudah dikesan jika sesuatu rekod diperkukuhkan bagi menjawab pertanyaan atau penyelesaian masalah.

6.3.13. Pemantauan Aktiviti Pelbagai

a. Selain daripada pemantauan kegunaan ID *Superuser*/ *Root*/ *Admin* dan ID Pentadbir (Sistem, Pangkalan Data, Keselamatan), beberapa aktiviti lain perlu juga dipantau. Pemantauan tersebut bergantung kepada tahap kritikal aplikasi dan sebagainya. Di antara aktiviti atau perkara yang perlu dipantau adalah:

   i. Kekerapan kegagalan sesuatu Logon ID,
   ii. Cubaan hak capaian yang tidak dibenarkan,
   iii. Perubahan data aplikasi (*before and after*),
   iv. Kegunaan kapasiti rangkaian.

b. Senarai tersebut hendaklah diluluskan oleh Pegawai Keselamatan ICT.

6.3.14. Penggunaan Peranti Peribadi

a. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada Jabatan. Walau bagaimanapun, peranti pengkomputeran peribadi milik pensendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan

dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

Seksyen 7. Kawalan Capaian Logikal

7.1. Tujuan dan Skop

Tujuan polisi 'Kawalan Capaian Logikal' adalah untuk menguatkuasakan pengasingan tugas dan memastikan individu yang diberi tanggungjawab mempunyai akauntabiliti ke atas akses untuk melaksanakan fungsi tersebut. Polisi ini berkaitan dengan kemudahan pemprosesan maklumat di bawah kawalan setiap Jabatan.

Tujuan prosedur Kawalan Capaian Logikal ini adalah untuk memastikan bahawa semua capaian aplikasi atau sistem dilakukan dengan terkawal dan kelulusan tertentu.

7.2. Pernyataan Polisi

Capaian kepada aplikasi atau sistem dan kemudahan yang berkaitan hendaklah dikawal dengan mengambil kira perundangan untuk melindungi data atau perkhidmatan;

Pengguna yang diberi hak capaian hendaklah memastikan mereka menggunakan hak dan tanggungjawab yang dibenarkan sahaja; dan Pengguna mesti melaporkan kepada pihak pengurusan apabila berlaku perubahan fungsi kerja.

7.3. Standard dan Prosedur Kawalan Capaian Logikal

7.3.1. Kawalan Capaian Logikal Secara Umum

a. Semua sistem atau aplikasi perlu mempunyai garispanduan capaian logikal yang memaparkan keperluan atau kategori pengguna dan hak capaian yang berpatutan. Hak capaian pada umumnya diberikan atas dasar keperluan (*need to know and need to use basis*);
b. Setiap pengguna, pentadbir dan penyelenggara aplikasi atau sistem akan diberi ID untuk memasuki aplikasi atau sistem serta hak capaiannya. Mereka yang diberi ID perlu memahami dan mematuhi syarat-syarat

penggunaan sistem dan juga keistimewaan hak capaian masing-masing dan memastikan semua ID dilindungi dari disalahguna atau dicerobohi;

c. ID umum sedia ada bagi aplikasi atau sistem seperti ID tetamu (*Guest*) atau ID tanpa identiti (*Anonymous*) perlu dipadamkan atau dikunci kegunaannya (*disable*) atau ditukar kata laluannya; dan

d. Setiap pengguna hendaklah memohon ID serta hak capaian dengan menggunakan Sistem KMS di Aduan Aplikasi.

7.3.2. Perlindungan Kata Laluan

a. Kata laluan mesti sekurang kurangnya mengandungi kombinasi dua belas (12) abjad dan nombor (*alphanumeric characters*);

b. Pengguna digalakkan menukarkan kata laluan sekurang-kurangnya setiap sembilan puluh (90) hari;

c. Kata laluan mesti ditukar dalam keadaan berikut:

i. Semasa memasuki sistem pertama (*first logon*) atau selepas sesuatu ID dipulihkan kegunaannya selepas penggantungan sementara;

ii. Kata laluan *default* yang dilengkapkan bersama aplikasi atau sistem yang dibekalkan;

iii. Apabila ID disyaki telah dicerobohi; dan

iv. Apabila berlaku pertukaran tugas.

d. Untuk aplikasi atau sistem dalam Kategori 1,

i. Kata laluan perlu dienkrip (*encrypted*); dan

ii. Aplikasi atau sistem perlu menentukan bahawa kata laluan hendaklah kukuh (*strong*) dan tidak mudah dikompromi. Antara kriteria yang boleh dikuatkuasakan ialah:

- Kata laluan tidak boleh sama dengan ID pengguna; dan

- Kata laluan tidak boleh mengguna perkataan-perkataan biasa dalam kamus.

e. Sistem hendaklah berkeupayaan untuk mengawal dan memantau panjangnya kata laluan dan kekerapan kata laluan perlu ditukar.

7.3.3. Pentadbiran ID dan Capaian Logikal

a. ID dan capaian logikal hanya boleh diberi selepas borang permohonan diisi dengan lengkap oleh pengguna, disokong atau disahkan oleh Pengurus pemohon, dan diluluskan oleh Pemilik Sistem atau Pemilik Data;
b. Pengguna-pengguna mesti memaklumkan kepada Pentadbir Keselamatan sekiranya mereka bertukar kerja atau berubah bidang tugas;
c. Setiap Jabatan/ Unit perlu menyediakan senarai terkini pengguna aplikasi atau sistem sekurang-kurangnya setahun sekali;
c. Pentadbir Keselamatan perlu menyemak dan menyelaras senarai terkini pengguna dan membandingkannya dengan borang permohonan dan pelupusan ID sekurang-kurangnya setahun sekali; dan
d. Untuk sistem dan aplikasi dalam Kategori 1, hak capaian untuk mengubah data dalam pangkalan data secara terus (*direct*) tidak dibenarkan sama sekali.

7.3.4. Pemansuhan Hak Capaian Logikal

a. Hak capaian pengguna yang tidak diperlukan lagi hendaklah dimansuhkan;
b. ID pengguna yang tidak aktif selama sembilan puluh (90) hari berturut-turut hendaklah dimansuhkan, kecuali ID yang memang dikenalpasti digunakan hanya pada masa tertentu; dan

c. Penggantungan ID perlu dikuatkuasakan secara automatik apabila berlaku tiga (3) kesalahan kata laluan berturut-turut. Pengguna hendaklah memohon untuk menggunakan ID itu kembali (*reactivated*). Peraturan ini hendaklah dilaksanakan bagi aplikasi baru yang ditauliahkan selepas tahun 2018.

7.3.5. Pemantauan Kegunaan Hak Capaian

a. Semua log atau *audit trail* hendaklah diaktifkan untuk merakamkan kegunaan ID dan hak capaian. Log tersebut perlu disemak oleh Pentadbir Keselamatan dari masa ke semasa untuk memastikan kegunaan sistem dengan betul dan teratur dan tidak ada unsur mencurigakan. Peraturan ini hendaklah dilaksanakan bagi aplikasi baru yang ditauliahkan selepas tahun 2018. Di antara perkara yang perlu diperhatikan ialah:
   i. Kegagalan memasuki sistem atau cubaan memasuki bahagian-bahagian aplikasi atau sistem yang diluar hak capaian pengguna berkenaan;
   ii. Kegunaan ID kritikal yang hak capaiannya luas; dan
   iii. Corak (*pattern*) kegunaan sistem yang luar biasa (contohnya luar dari waktu pejabat biasa).

b. **Untuk sistem dan aplikasi dalam Kategori 1 log atau Jejak Audit perlu diaktifkan untuk merekodkan kegunaan ID dan hak capaian.** Log ini perlu disemak oleh Pentadbir Keselamatan dari semasa ke semasa.

c. Hak capaian sementara dalam keadaan kecemasan (*emergency*) dan utiliti berkuasa (*powerful utilities*) hendaklah dikawal dan dipantau kegunaannya.

d. Penamatan secara automatik (*auto logoff*) perlu dilaksanakan untuk menamatkan aplikasi secara

automatik bagi pengguna yang tidak aktif (*idle*) selepas suatu tempoh masa yang telah ditetapkan iaitu selama 20 minit.

7.3.6. Kriptografi

a. Kriptografi merupakan alat yang penting dan asas untuk menguruskan keselamatan ICT.

b. Pentadbir Keselamatan perlu memastikan penggunaan kriptografi ke atas semua maklumat sensitif atau maklumat rahsia rasmi di jabatan . Contoh :

   i. Katalaluan

   ii. Secure Sockets Layer (SSL)

Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi

8.1. Tujuan dan Skop

Polisi 'Pembangunan dan Penyelenggaraan Aplikasi' memastikan Pembangunan dan Penyelenggaraan Aplikasi dibuat secara konsisten dan berstruktur supaya penambahan ciri-ciri dan fungsi dilaksanakan dengan terkawal dan teratur.

Polisi ini adalah berkaitan dengan kitarhayat pembangunan dan penyelenggaraan aplikasi. Manakala tujuan prosedur adalah untuk memastikan bahawa pembangunan aplikasi dan penyelenggaraan aplikasi dijalankan dengan betul untuk menjamin keselamatan aplikasi.

8.2. Pernyataan Polisi

Aplikasi yang dibangunkan dan dibekalkan hendaklah sentiasa mengikut proses pembangunan formal yang mesti diurus dan disokong dengan kawalan perubahan, pengurusan konfigurasi dan pengurusan pengeluaran *(patch)* yang sesuai.

Kawalan yang sesuai hendaklah dibangunkan untuk aplikasi bagi memastikan integriti dan kerahsiaan maklumat yang dimasukkan, diproses dan disimpan dilindungi sepenuhnya.

Keteguhan kawalan keselamatan aplikasi hendaklah diuji dari semasa ke semasa.

8.3. Standard dan Prosedur Pembangunan dan Penyelenggaraan Aplikasi

8.3.1. Prosedur Pembangunan Aplikasi

Pembangunan aplikasi hendaklah berpandukan metodologi seperti:

a. Analisis: Kenalpasti masalah sistem dan penambahbaikan yang perlu dilakukan
b. Rekabentuk: Proses mereka bentuk sistem
c. Pembangunan: Proses pembangunan sistem dilaksanakan
d. Pengujian: Menguji kefungsian sistem

e. Pelaksanaan: Sistem telah sedia digunakan

f. Penyelenggaraan: Menyelenggara masalah berkaitan sistem

8.3.2. Spesifikasi Keselamatan Dalam Aplikasi

a. Aplikasi hendaklah dibangunkan dengan mengambil kira keperluan keselamatan semasa fasa spesifikasi dan rekabentuk. Keselamatan tersebut merangkumi aspek kerahsiaan, integriti dan ketersediaan;

b. Kajian hendaklah dibuat untuk mengenalpasti ciri-ciri kelemahan yang sedia ada dalam perisian asas dan cara untuk mengatasinya dan seterusnya pastikan bahawa langkah-langkah tersebut dilaksanakan dalam aplikasi dengan betul;

c. Rekabentuk sistem hendaklah mempunyai ciri mesra pengguna (*user friendly*) supaya sistem mudah difahami oleh setiap peringkat pengguna;

d. Ciri keselamatan sistem perlu ada dalam pembangunan sistem bagi mengawal ketepatan dan integriti data. Antaranya:

   i. Penyimpanan data kata laluan ke dalam pangkalan data perlu dienkripsi bagi menjamin keselamatan maklumat pengguna;

   ii. Data perlu disahkan (*validate*) semasa peringkat kemasukan atau perubahan data bagi mengawal ketepatan dan integritinya; Pengesahan (*validation*) merangkumi format medan (*field format*) untuk tarikh atau angka yang diwajibkan kemasukannya dengan had lingkungan yang ditetapkan (*valid data range*);

   iii. Penghapusan data dilakukan selepas pengenalpastian data yang ingin dihapus selepas peringatan diberi untuk mengawal ketepatan dan integritinya; dan

iv. Aplikasi hendaklah berupaya menjana *audit trails* bagi transaksi penting dalam aktiviti kemasukan data, perubahan data dan penghapusan data.

e. Aplikasi hendaklah diuji dari aspek fungsi dan keselamatannya manakala semua kawalan keselamatan yang merangkumi kombinasi kawalan teknikal dan prosedur (*technical and procedural controls*) perlu didokumentasikan. Aspek-aspek keselamatan tersebut hendaklah dimaklumkan kepada pengguna aplikasi Sistem;

f. Aplikasi hendaklah berupaya menjana *audit trails* bagi transaksi penting dalam aktiviti:

i. Kemasukan data;

ii. Perubahan data; dan

iii. Penghapusan data.

g. Data perlu disahkan (*validat*e) semasa peringkat kemasukan atau perubahan data bagi mengawal ketepatan dan integritinya. Pengesahan (*validation*) merangkumi format medan (*field format*) untuk tarikh atau angka yang diwajibkan kemasukannya dengan had lingkungan yang ditetapkan (*valid data range*); dan

h. Penghapusan data dilakukan selepas pengenalpastian data yang ingin dihapus selepas peringatan diberi untuk mengawal ketepatan dan integritinya.

8.3.3. Pembangunan dan Penyelenggaraan Aplikasi

a. Penerima aplikasi atau Pemilik Data hendaklah memastikan bahawa:

i. Pembangunan aplikasi mengikut pengurusan projek dan kawalan kualiti yang mantap;

ii. Keperluan pelaksanaan aplikasi didokumentasikan;

iii. Perubahan aplikasi dikawal dengan baik dan direkodkan;

iv. Paparan amaran dan makluman hendaklah dipamerkan bila perlu (*context sensitive warning, error or help messages*);

v. Penyemakan integriti (*integrity checks*) dilaksanakan di bahagian-bahagian perisian yang berpatutan;

v. Proses ujian aplikasi dilakukan dengan sempurna dan menyeluruh;

vi. Latihan pengguna disediakan; dan

vii. Dokumentasi pemasangan, kegunaan, pembetulan dan senggaraan aplikasi disediakan.

Seksyen 9. Pengurusan Insiden

9.1. Tujuan dan Skop

Polisi 'Pengurusan Insiden' bertujuan untuk menetapkan kaedah rasmi bagi mengurus masalah supaya semua aduan didaftar, disiasat dan diselesaikan dalam masa yang ditetapkan mengikut piagam pelanggan.

Polisi ini berkaitan dengan kemudahan pemprosesan maklumat di bawah kawalan setiap Jabatan/ Unit. Manakala prosedur adalah untuk menghuraikan langkah-langkah untuk melaporkan insiden atau masalah dan urutan tindakan penyelesaian masalah.

9.2. Pernyataan Polisi

Pentadbir Sistem hendaklah memastikan semua aduan didaftar, disiasat dan diselesaikan secara terkawal dan tepat. Semua masalah atau insiden yang didaftarkan hendaklah disemak dan dipantau secara berkala oleh pihak pengurusan.

Setiap pengguna hendaklah mengamalkan kaedah penggunaan ICT yang betul dan selamat dari semasa ke semasa. Sebarang masalah dan kejadian luarbiasa termasuk serangan virus atau *worm*, penurunan prestasi sistem atau penjejasan keselamatan hendaklah dilaporkan.

9.3. Standard dan Prosedur Pengurusan Insiden

9.3.1. Laporan Insiden dan Penyelesaian

a. Setiap insiden hendaklah dilaporkan menggunakan Sistem KMS di Aduan Aplikasi **dan perlu dilaporkan secara rasmi kepada JTM**.

b. Peruntukkan setiap insiden kepada kakitangan bantuan bertugas untuk penyelesaian mengikut prioriti,

c. Meja bantuan hendaklah mengagihkan setiap insiden kepada kakitangan bantuan yang bertugas untuk penyelesaian mengikut prioriti;
d. Kakitangan bantuan yang bertugas perlu merangka tindakan pembetulan yang sesuai untuk menyelesaikan masalah atau insiden;
e. Semua yang terlibat menyelesaikan sesuatu insiden hendaklah bekerjasama dan berhubung rapat untuk menyelesaikan insiden tersebut; dan
f. Sekiranya penyelesaian insiden adalah di luar bidang tugas atau bidang pengalaman kakitangan bantuan, maka laporan insiden tersebut hendaklah dimajukan ke peringkat lebih tinggi.
g. Bagi insiden keselamatan yang melibatkan serangan siber, SOP Pengurusan Pengendalian Insiden Keselamatan ICT Jabatan/ Unit masing-masing perlu dipatuhi jika ada.

9.3.2. Pemantauan Penyelesaian Laporan Insiden

a. Semua laporan perlu dipantau tahap atau peringkat penyelesaiannya dan tindakan susulan perlu diambil untuk menyelesaikan insiden yang serius secepat mungkin.
b. Insiden keselamatan siber yang melibatkan Maklumat Rahsia Rasmi hendaklah dirujuk kepada CGSO untuk tindakan selanjutnya.
c. Kajian perlu dilakukan dari semasa ke semasa untuk mengenalpasti corak atau *trend* laporan insiden dan merangka penyelesaian jangka masa panjang supaya insiden tidak berulang.

Seksyen 10. Pengurusan Kesinambungan Perkhidmatan

10.1. Tujuan dan Skop

'Pengurusan Kesinambungan Perkhidmatan (PKP)' menyediakan kerangka pengurusan (*management framework*) untuk memulihkan perkhidmatan secara formal supaya Jabatan/ Unit dapat meneruskan operasi sekiranya berlaku gangguan ICT yang berpanjangan. PKP hendaklah diurus dan dirangka dengan tepat dengan perbelanjaan yang berpatutan.

Polisi ini dikuatkuasakan ke atas semua sistem dalam **Kategori 1** di bawah kawalan Jabatan/ Unit berdasarkan penilaian risiko dalam Pengurusan Kesinambungan Perkhidmatan.

10.2. Penyataan Polisi

Pengurusan Kesinambungan Perkhidmatan hendaklah diwujudkan bagi menjamin kesinambungan perkhidmatan yang berkaitan dengan proses kerja yang disokong oleh sistem dalam Kategori 1.

10.3. Standard dan Prosedur Pengurusan Kesinambungan Perkhidmatan

10.3.1. Kewajipan Merangka Kesinambungan Perkhidmatan

a. Pihak pengurusan hendaklah mewujudkan satu (1) jawatankuasa khusus untuk merancang dan membangunkan Pelan Kesinambungan Perkhidmatan (PKP). Tugas dan tanggungjawab jawatankuasa tersebut hendaklah dikenalpasti dan dipersetujui;
b. Kakitangan-kakitangan yang terlibat hendaklah terdiri daripada mereka yang berpengalaman dan memahami konteks perkhidmatan dan keperluan kesinambungan perkhidmatan; dan
c. Kemajuan rancangan hendaklah dipantau.

10.3.2. Analisa Dan Mengenalpasti Perkhidmatan Kritikal

a. Proses atau metodologi yang diiktiraf perlu digunakan untuk mengenalpasti perkhidmatan-perkhidmatan kritikal dan prosedurbaikpulih perkhidmatan hendaklah diperincikan apabila berlaku gangguan;

b. Perkhidmatan penting hendaklah diperincikan dari segi impak gangguan (*Business Impact Analysis*), analisa risiko kemungkinan gangguan akibat kelemahan dan ancaman (*Risk Assessment*) dan pembangunan strategi pemulihan (*Recovery Strategies*); dan

c. Perkhidmatan yang penting hendaklah dikenalpasti dan prosedur pemulihan perkhidmatan hendaklah diperincikan apabila berlaku gangguan.

10.3.3. Pelaksanaan Pelan dan Ujian

a. Pelan kesinambungan perkhidmatan dan Pelan Pemulihan Bencana ICT (ICT DRP) perlu dirangka dan diuji kesesuaian dan ketepatannya dari semasa ke semasa;

b. Dokumen pelan kesinambungan perkhidmatan dan Pelan Pemulihan Bencana ICT (ICT DRP) perlu dikemas kini dari semasa ke semasa dan diedarkan kepada semua yang berkaitan;

c. Semua yang berkaitan hendaklah dilatih untuk melaksanakan bidang tugas masing-masing apabila berlaku gangguan perkhidmatan yang memerlukan pelan kesinambungan perkhidmatan atau Pelan Pemulihan Bencana ICT (ICT DRP) diaktifkan;

d. Ujian pemulihan ICT hendaklah dilakukan lebih kerap dari ujian keseluruhan; dan

e. Hasil ujian untuk analisa dan rancangan pembetulan prosedur hendaklah didokumenkan.

Seksyen 11. Pematuhan

11.1. Tujuan dan Skop

Polisi 'Pematuhan' ini menggariskan kawalan dan langkah-langkah untuk:

- Menghindar dari melanggar sebarang undang-undang jenayah dan sivil, keperluan pihak berkuasa, peraturan, perjanjian dan juga lain-lain keperluan keselamatan;
- Memastikan pematuhan dan pengamalan Polisi Keselamatan ICT; dan
- Memaksimumkan keberkesanan pelaksanaan keselamatan dan mengurangkan gangguan sistem.

Polisi ini berkaitan dengan pelaksanaan keseluruhan sistem di bawah kawalan setiap Jabatan/ Unit.

11.2. Pernyataan Polisi

Rekabentuk, operasi, penggunaan dan pengurusan sistem maklumat mungkin tertakluk kepada keperluan pihak berkuasa, peraturan, perjanjian dan juga lain-lain keperluan keselamatan. Keperluan perundangan spesifik hendaklah dirujuk kepada Penasihat Undang-Undang Kerajaan.

Polisi Keselamatan, Standard dan Prosedur hendaklah disemak dari semasa ke semasa.

11.3. Standard dan Prosedur Pematuhan

11.3.1. Pematuhan Kepada Keperluan Undang Undang

a. Keperluan undang-undang, peraturan-peraturan serta arahan atau garis panduan Kerajaan perlu dikenalpasti untuk pematuhan dalam kegunaan aplikasi atau sistem supaya Kerajaan tidak terbuka kepada tindakan undang-undang oleh pihak ketiga. Ini termasuk keperluan pematuhan

dari segi kerahsiaan maklumat, tempoh simpanan rekod, ketepatan maklumat dan langkah-langkah keselamatan yang lain untuk melindungi maklumat;

b. Khidmat nasihat berkaitan undang undang dan garis panduan yang berkaitan dengan operasi Jabatan/ Unit hendaklah dikaji dan diambil jika perlu; dan
c. Langkah untuk mematuhi keperluan undang-undang, peraturan-peraturan serta arahan atau garis panduan Kerajaan hendaklah diaturkan.

11.3.2. Semakan Polisi, Standard dan Prosedur Dan Pematuhan

a. Polisi, Standard dan Prosedur hendaklah disemak dan dikemaskini dari masa ke masa untuk menentukan ia menepati keperluan semasa dan akan datang;
b. Semua Ketua Jabatan/ Unit hendaklah memastikan bahawa Polisi, Standard dan Prosedur dipatuhi oleh kakitangan di jabatan/ Unit masing-masing dan merangka pelan untuk mengukur tahap pematuhan Polisi Keselamatan Jabatan/ Unit.

11.3.3. Keperluan Audit

a. Audit dalaman dan luaran hendaklah dilakukan dari semasa ke semasa ke atas amalan penggunaan, pentadbiran dan penyelenggaraan aplikasi dan sistem tersebut. Ini bertujuan untuk memastikan tahap pematuhan yang jitu dan bagi mengenalpasti kelemahan-kelemahan amalan keselamatan dan membuat teguran yang sewajarnya kepada Jabatan/ Unit.
b. Semua rekod aktiviti dan rekod semakan yang disimpan dalam simpanan rekod hendaklah dipastikan

disimpan dengan baik dan teratur supaya senang dicapai untuk kajian atau untuk tujuan audit.

11.3.4. Audit Dalaman dan Luaran

a. Juru Audit Jabatan/ Unit adalah fungsi sampingan antara kakitangan terlatih dalam Jabatan/ Unit yang mengendalikan aplikasi. Di antara fungsinya adalah:

   i. menjalankan audit pemantauan dalam Jabatan/ Unit dari semasa ke semasa;
   ii. tidak perlu terdiri daripada kalangan teknikal ICT tetapi hendaklah orang terlatih yang boleh memahami dan mematuhi keperluan polisi, standard atau prosedur, serta merekodkan hasil kajiannya untuk perhatian dan tindakan pengurusan Jabatan/ Unit;
   iii. tidak perlu menjalankan audit serentak untuk semua bahagian berkaitan ICT Jabatan/ Unit, tetapi digalakkan untuk dipecahkan kepada bahagian tertentu (contoh: pengurusan rangkaian atau pengurusan semakan log sistem) untuk diaudit pada sesuatu masa; dan

b. Juru Audit Dalaman adalah dari kakitanga MPAG dan menjalankan audit berjadual; dan
c. Perunding yang berkemampuan hendaklah digunakan untuk menjalankan Audit Luaran terhadap polisi, standard dan prosedur keselamatan ICT.

11.3.5. Hak Capaian Untuk Juru Audit

a. Hak capaian sementara yang terhad dan terkawal boleh diberi kepada Juru Audit, sekiranya terdapat keperluan dan perlu dimansuhkan setelah digunakan dalam tempoh audit.