POLISI DAN STANDARD KESELAMATAN ICT

NEGERI MELAKA

Versi 1.5 :: Dis 2015

KANDUNGAN

PENGENALAN DOKUMEN iv
I. PENGENALAN xi
II. PERNYATAAN DASAR KESELAMATAN ICT NEGERI Melaka xii
III. OBJEKTIF KESELAMATAN ICT NEGERI Melaka xiv
IV. PRINSIP KESELAMATAN ICT NEGERI MELAKA xv
V. SKOP POLISI KESELAMATAN ICT NEGERI MELAKA xvii
VI. DOKUMEN RUJUKAN xviii
VII. HIERARKI DAN HUBUNG KAIT DOKUMEN xix
VIII. KATEGORI SISTEM DAN APLIKASI DI KERAJAAN NEGERI MELAKA xx
IX. TANGGUNGJAWAB xxii
X. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN xxiii
XI. PENERANGAN TERMINOLOGI FUNGSI xxiv
XII. DEFINISI POLISI, STANDARD DAN PROSEDUR 1
XIII. POLISI KESELAMATAN ICT NEGERI MELAKA 2
Seksyen 1. Polisi Keselamatan Maklumat 2
1.1. Tujuan dan Skop 2
1.2. Pernyataan Polisi 2
Seksyen 2. Pengurusan Keselamatan Maklumat 3
2.1. Tujuan dan Skop 3
2.2. Pernyataan Polisi 3
2.3. Standard Pengurusan Keselamatan Maklumat 3
2.4. Hubung kait Pengurusan Maklumat 3
2.5. Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka 7
2.6. Ketua Pegawai Maklumat 7
2.7. Pegawai Keselamatan ICT 8
2.8. Pemilik Aset 8
2.9. Penjaga atau Pengguna Aset 9
2.10. Pemilik Aplikasi/Sistem 9
2.11. Pengurus Aplikasi/Sistem 9
2.12. Pemilik Data 10
2.13. Pentadbir Aplikasi/Sistem 11
2.14. Pentadbir Pangkalan Data 11
2.15. Pentadbir Keselamatan 12
2.16. Penyelaras Prosedur 12
2.17. Ketua Jabatan/Pegawai Pengawal 13
2.18. Pengguna-Pengguna 13
2.19. Khidmat Bantuan Tahap 1 14
2.20. Khidmat Bantuan Tahap 2 14
2.21. Juru Audit Jabatan 15

2.22. Juru Audit Dalaman 15
2.23. Juru Audit Luaran 15
Seksyen 3. Pengurusan Aset Berkaitan Maklumat 16
3.1. Tujuan dan Skop 16
3.2. Pernyataan Polisi 16
3.3. Standard Pengurusan Aset 16
Seksyen 4. Keselamatan Sumber Manusia 18
4.1. Tujuan dan Skop 18
4.2. Pernyataan Polisi 18
4.3. Standard Keselamatan Sumber Manusia 18
4.3.1. Tanggungjawab Kakitangan 18
4.3.2. Penjawatan Kakitangan 18
4.3.3. Latihan Kesedaran Keselamatan Maklumat 19
4.3.4. Kewajipan Kakitangan dan Tindakan Disiplin 19
4.3.5. Pengendalian Kakitangan Yang Berpindah Atau Bersara 20
4.3.6. Tindakan Kakitangan Terhadap Insiden Keselamatan 20
Seksyen 5. Kawalan Fizikal dan Persekitaran 21
5.1. Tujuan dan Skop 21
5.2. Pernyataan Polisi 21
5.3. Standard Kawalan Fizikal Dan Persekitaran 21
5.3.1. Keperluan Umum 21
5.3.2. Kawalan Keselamatan Fizikal 22
5.3.3. Kawalan Media Storan 22
Seksyen 6. Pengurusan Operasi dan Rangkaian 23
6.1. Tujuan dan Skop 23
6.2. Pernyataan Polisi 23
6.3. Standard Pengurusan Operasi dan Rangkaian 24
6.3.1. Pengurusan Konfigurasi 24
6.3.1.1. Pengurusan Konfigurasi Sistem 24
6.3.1.2. Pengurusan Konfigurasi Rangkaian 25
6.3.1.3. Perubahan Konfigurasi Sementara 26
6.3.1.4. Perubahan Konfigurasi Dalam Keadaan Kecemasan 27
6.3.2. Pengasingan Kerja 27
6.3.3. Kawalan Kegunaan ID Hak Capaian Tinggi 28
6.3.4. Prosedur Operasi (Operating Procedures) dan Dokumentasi 28
6.3.5. Senggaraan Aplikasi atau Sistem 29
6.3.6. Perjanjian Tahap Perkhidmatan 29
6.3.7. Backup dan Media Backup 30
6.3.8. Komputer Kerajaan Negeri 31
6.3.9. Rangkaian Tanpa Wayar 31
6.3.10. Perancangan Kapasiti Perkakasan 32
6.3.11. Simpanan Rekod dan Pengurusan Kualiti 32

Seksyen 7. Kawalan Capaian Logikal 33
7.1. Tujuan dan Skop 33
7.2. Pernyataan Polisi 33
7.3. Standard Kawalan Capaian Logikal 33
7.3.1. Kawalan Capaian Logikal Secara Umum 33
7.3.2. Perlindungan Kata Laluan 34
7.3.3. Pentadbiran ID dan Capaian Logikal 35
7.3.4. Pemansuhan Hak Capaian Logikal 35
7.3.5. Pemantauan Kegunaan Hak Capaian 36
Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi 37
8.1. Tujuan dan Skop 37
8.2. Pernyataan Polisi 37
8.3. Standard Pembangunan dan Penyelenggaraan Aplikasi 37
8.3.1. Spesifikasi Keselamatan Dalam Aplikasi 37
8.3.2. Pembangunan dan Penyelenggaraan Aplikasi 38
Seksyen 9. Pengurusan Insiden 40
9.1. Tujuan dan Skop 40
9.2. Pernyataan Polisi 40
9.3. Standard Pengurusan Insiden 40
9.3.1. Laporan Insiden dan Penyelesaian 40
9.3.2. Pemantauan Penyelesaian Laporan Insiden 41
Seksyen 10. Pengurusan Kesinambungan Perkhidmatan 42
10.1. Tujuan dan Skop 42
10.2. Penyataan Polisi 42
10.3. Standard Pengurusan Kesinambungan Perkhidmatan 42
10.3.1. Kewajipan Merangka Kesinambungan Perkhidmatan 42
10.3.2. Analisa Dan Mengenalpasti Perkhidmatan Kritikal 42
10.3.3. Perlaksanaan Pelan dan Ujian 43
Seksyen 11. Pematuhan 44
11.1. Tujuan dan Skop 44
11.2. Pernyataan Polisi 44
11.3. Standard Pematuhan 44
11.3.1. Pematuhan Kepada Keperluan Undang Undang 44
11.3.2. Semakan Polisi dan Standard Dan Pematuhan 45
11.3.3. Keperluan Audit 45
11.3.4. Hak Capaian Untuk Juru Audit 45
LAMPIRAN 1

PENGENALAN DOKUMEN

NAMA DOKUMEN	**:**	**Polisi dan Standard Keselamatan ICT Negeri Melaka**
VERSI	**:**	**1.5**
TARIKH	**:**	**Disember 2015**

LOG KAWALAN KEMAS KINI DOKUMEN

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
1.	21/08/2009	VIII. Kategori Sistem dan Aplikasi di Kerajaan Negeri Melaka	Tambahan kepada Sistem dan Aplikasi Kritikal – Kategori 1
2.	29/10/2010	Seksyen 6. Pengurusan Operasi dan Rangkaian	Tambahan kepada perenggan di para 6.2 Pernyataan Polisi dan para 6.3.9 Rangkaian Tanpa Wayar
3.	5/6/2012	I. Pengenalan	Tambahan kepada perenggan di mukasurat vii
		VIII.Kategori Sistem Dan Aplikasi Di Kerajaan Negeri Melaka	Menggugurkan perenggan di mukasurat xviii
		IX.Tanggungjawab	Pindaan Jawatankuasa
		X.Pengemaskinian Dan Penyenggaraan Dokumen	Pindaan Jawatankuasa Pindaan No.Telefon Tambahan keterangan *
		XI.Penerangan Terminologi Fungsi	Pindaan fungsi Jawatankuasa Tambahan fungsi Ketua Pegawai Maklumat (CIO).
		Seksyen 2. Pengurusan Keselamatan Maklumat	Pindaan Rajah 1 : Hubung kait Pengurusan Keselamatan Maklumat Pindaan Jawatankuasa di para 2.3.1 Pindaan *Intrusion Detection Systems (IDS)* dan *Intrusion Protection Systems (IPS) di para 2.3.1* Pindaan Pusat Data di para 2.3.1 Pindaan Jawatankuasa di para 2.3.2 Tambahan Ketua Pegawai Maklumat (CIO) di para 2.3.3
		Seksyen 3. Pengurusan Aset Berkaitan	Pindaan Pusat Data di para 3.1

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		Maklumat	
		Seksyen 5. Kawalan Fizikal dan Persekitaran	Pindaan Pusat Data di para 5.3.1 dan 5.3.2
		Seksyen 10. Pengurusan Kesinambungan Perkhidmatan	Pindaan tujuan dan skop di para 10.1
4.	22 Julai 2014	IV. PRINSIP KESELAMATAN ICT NEGERI MELAKA	Pindaan di para 6: Pelan Pemulihan Bencana ICT
		VIII. KATEGORI SISTEM DAN APLIKASI DI KERAJAAN NEGERI MELAKA	• Pindaan Jadual 1: ○ E-ADUAN kepada Sistem Pengurusan Aduan Bersepadu Kerajaan Negeri Melaka (SISPAA) ○ Portal EPG kepada Gerbang Pembayaran Bersepadu Kerajaan Negeri Melaka (e-Bayar) • Menggugurkan *Generic Office Environment* – Electronic *Government Document Management System* (GOE-EGDMS) dari Jadual 1
		X. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN	• Pindaan Bahagian Perkhidmatan Teknologi Maklumat kepada Bahagian Teknologi Maklumat dan Komunikasi (BTMK) • Pindaan BPTM kepada BTMK • Pindaan Pengarah kepada Ketua ICT Negeri
		Seksyen 2. Pengurusan Keselamatan Maklumat	• Pindaan Bahagian Perkhidmatan Teknologi Maklumat kepada Bahagian Teknologi Maklumat dan Komunikasi • Pindaan BPTM kepada BTMK

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			• Tambahan perenggan di para 2.3: Manakala maklumat milik kerajaan perlu disimpan di premis milik kerajaan dan diuruskan oleh kakitangan kerajaan. • Pindaan di para 2.3.18: Juru Audit Jabatan bertanggungjawab melaksanakan audit pemantauan terhadap sistem dan proses pengurusan keselamatan ICT • Pindaan di para 2.3.19: Juru Audit Dalaman bertanggungjawab mengaudit sistem dan proses pengurusan keselamatan ICT di seluruh Jabatan bagi mempastikan tahap pematuhan Polisi dan Standard Keselamatan ICT dan mencadangkan langkah-langkah pembetulan. • Pindaan di para 2.3.20: Juru Audit Luaran bertanggungjawab mengaudit sistem dan proses pengurusan keselamatan ICT di Jabatan untuk mempastikan tahap pematuhan Polisi dan Standard Keselamatan ICT dan melaporkan teguran-teguran jika terdapat ketidakpatuhan.
		Seksyen 3. Pengurusan Aset Berkaitan Maklumat	• Pembetulan ejaan cekera kepada cakera
		Seksyen 4. Keselamatan Sumber Manusia	• Pindaan di para 4.3.5.b: Kata laluan bagi pengguna berkenaan hendaklah diubah selepas tarikh perpindahan atau persaraan kakitangan berkenaan dan Logon IDnya digantung dalam tempoh tiga bulan sebelum dimansuhkan
		Seksyen 5. Kawalan Fizikal dan	• Pembetulan ejaan mempamirkan kepada mempamerkan

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		Persekitaran	• Pembetulan frasa 'masa ke semasa' kepada 'semasa ke semasa'
		Seksyen 6. Pengurusan Operasi dan Rangkaian	• Pembetulan di para 6.3.1.1.a.ii: Dikemaskinikan rekodnya apabila berlaku perubahan, penukaran atau naiktaraf • Pembetulan di para 6.3.1.2.e.i: Keperluan memaklumkan dan mendapat kelulusan seperti di perenggan 6.3.1.1-b wajib dipatuhi • Pembetulan di para 6.3.4a.iii: Backup and Recovery • Pembetulan frasa 'dari masa ke semasa' kepada 'dari semasa ke semasa' • Pindaan BPTM kepada BTMK
		Seksyen 7. Kawalan Capaian Logikal	• Menggugurkan kriteria 'Kata laluan tidak boleh mengguna abjad yang sama (repeating characters)' di para 7.3.2.d.ii
5.	4 Disember 2015	VIII. Kategori Sistem dan Aplikasi di Kerajaan Negeri Melaka	• Kemaskini Jadual 1: Sistem atau Aplikasi Penting dan Kritikal - Kategori 1
		XI. Penerangan Terminologi Fungsi	• Pindaan di Jadual 2: Terminologi Fungsi dan Bidang Tugas: ○ Perubahan kedudukan senarai fungsi CIO dan ICTSO ○ Pindaan keterangan di fungsi Juru Audit Dalaman ○ Pindaan keterangan di fungsi Pengurus Aplikasi/ Sistem"
		XII. Definisi Polisi, Standard dan Prosedur	• Pindaan frasa di para 2. • Hapuskan perenggan kedua di para 3.

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		Seksyen 2. Pengurusan Keselamatan Maklumat	• Pembetulan frasa di para 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.20, 2.21, 2.22 dan 2.23 • Pindaan di para 2.4: ○ "Sistem Pendaftaran Tanah Berkomputer (SPTB)" kepada "Sistem e-Tanah" ○ Hapus "(SUK)" pada Rajah 1: Hubung kait Pengurusan Keselamatan Maklumat • Pindaan "ISP" kepada (PSICT) di para 2.6(a) • Pindaan "SPTB" kepada "e-Tanah" di para 2.10 • Hapuskan frasa "data/bahagian" dan "seperti masuk, semaka, lulus, melihat dan lupus data" di para 2.12(a) • Hapuskan perenggan "Juru audit Dalaman terdiri daripada kakitangan Audit SUK" di para 2.22
		Seksyen 3. Pengurusan Aset Berkaitan Maklumat	• Penambahan *"centralised uninterruptible power supply* dan*"* para 3.1 (b) • Pembetulan frasa di para 3.2 dan 3.3
		Seksyen 4. Keselamatan Sumber Manusia	• Pembetulan frasa di para 4.2, 4.3.2, 4.3.4 dan 4.3.5
		Seksyen 5. Kawalan Fizikal dan Persekitaran	• Hapuskan perkataan "bilik UPS" di para 5.3.1 (a) • Pembetulan frasa di para 5.3.1(c)
		Seksyen 6. Pengurusan Operasi dan Rangkaian	• Pembetulan frasa di para 6.3.1.1(v) dan 6.3.7

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			• Pembetulan frasa di para 6.2 • Pembetulan frasa di para 6.3.9 • Pembetulan frasa dan penambahan perenggan "melalui penggunaan suatu sistem pemantauan perkakasan dan rangkaian serta hasil penyelenggaraan berkala peralatan ICT di BTMK" di para 6.3.10 (a) ii
		Seksyen 7. Kawalan Capaian Logikal	• Pindaan "lapan (8)" kepada "dua belas (12)" di para 7.3.2 (a) • Pembetulan frasa di para 7.3.3(c) dan 7.3.4(b)
		Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi	• Penambahan perenggan "Penghapusan data dilakukan selepas pengenalpastian data yang ingin dihapus selepas peringatan diberi untuk mengawal ketepatan dan integritinya." selepas para 8.3.1(d)
		Seksyen 9. Pengurusan Insiden	• Pembetulan frasa di para 9.1 dan 9.2,
		Seksyen 10. Pengurusan Kesinambungan Perkhidmatan	• Pembetulan frasa di para 10.1, 10.2, 10.3.1, 10.3.2, 10.3.3.
		Seksyen 11. Pematuhan	• Pembetulan frasa di para 11.1, 11.3.2, 11.3.3 dan 11.3.4

I. PENGENALAN

Dokumen ini, Polisi dan Standard Keselamatan ICT Negeri Melaka (Polisi dan Standard), menggariskan **polisi minimum** yang perlu dipatuhi oleh Pengurusan dan kakitangan berkaitan dengan penggunaan dan pengurusan ICT di semua Jabatan Kerajaan Negeri Melaka (Kerajaan Negeri). Walau bagaimanapun, jabatan/agensi boleh menggunapakai Dasar Keselamatan ICT masing-masing mengikut kesesuaian.

II. PERNYATAAN DASAR KESELAMATAN ICT NEGERI MELAKA

1. Dasar Kerajaan Negeri Melaka 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 Polisi dan Standard menjamin tahap perlindungan dari berlakunya insiden pencerobohan keselamatan. Ia juga menyediakan respons serta tindakan keselamatan ICT apabila pencerobohan berlaku.
5. Polisi dan Standard 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. Polisi dan Standard akan mengurangkan ketidaktentuan, persoalan dan ketidakseragaman di dalam mengurus dan menggunakan ICT.

III. OBJEKTIF KESELAMATAN ICT NEGERI MELAKA

Objektif keselamatan adalah seperti berikut:

a) Menyediakan prinsip panduan minimum untuk pengurusan yang selamat dan sesuai, penggunaan dan pengoperasian sistem dan aplikasi;
b) 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;
c) Menyediakan panduan untuk tindakan pembetulan sekiranya berlaku pencerobohan keselamatan atau ketidakpatuhan yang serius;
d) 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
e) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

IV. PRINSIP KESELAMATAN ICT NEGERI MELAKA

Polisi Keselamatan ICT Negeri Melaka 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

Polisi dan Standard hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk percanggahan yang boleh mendatangkan ancaman kepada keselamatan Kerajaan Negeri Melaka.

V. SKOP POLISI KESELAMATAN ICT NEGERI MELAKA

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

Polisi dan Standard ini adalah arahan tahap tinggi yang menentukan bagaimana aset ICT diurus, dilindungi dan disebarkan kepada semua Jabatan/ Agensi. Pelaksanaan Polisi dan Standard ini adalah wajib dan setiap Jabatan/ Agensi 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 Polisi dan Standard perlu dipatuhi.

VI. DOKUMEN RUJUKAN

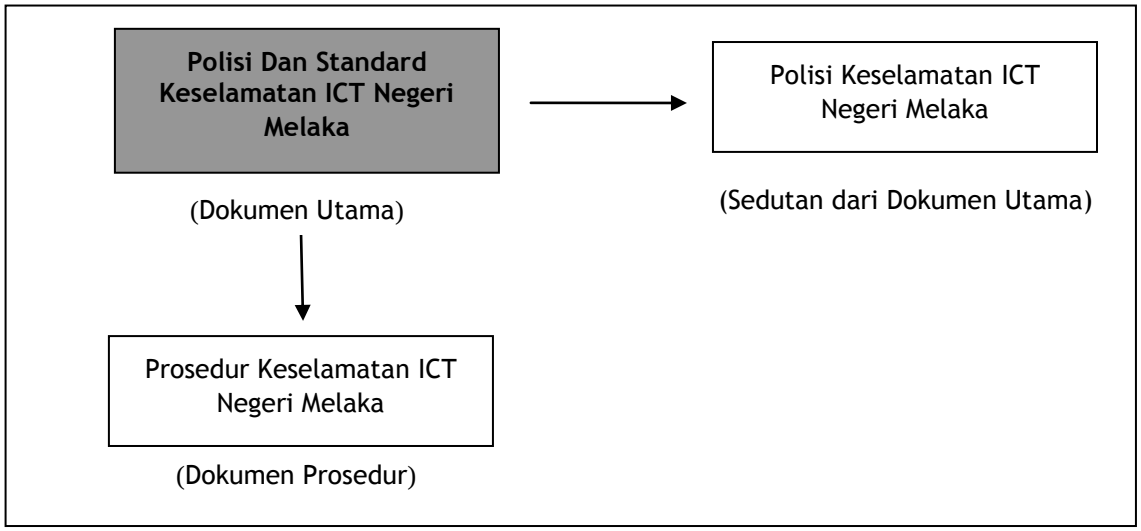
Berikut adalah dokumen-dokumen yang dirujuk semasa penyediaan dokumen ini:

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; dan
k) Arahan Perbendaharaan.

VII. HIERARKI DAN HUBUNG KAIT DOKUMEN

Dokumen ini adalah merupakan dokumen utama yang mengandungi polisi dan standard pengurusan keselamatan maklumat, operasi dan penggunaan sistem dan aplikasi.

Dokumen Polisi Keselamatan ICT adalah intipati dari dokumen utama yang dijadikan sebagai rujukan. Bagi menyokong pelaksanaan Polisi dan Standard ini, langkah-langkah terperinci telah dibangunkan sebagai Prosedur Keselamatan ICT Jabatan/ Agensi. Hubung kait keseluruhan dokumen adalah seperti Gambarajah 1:



Gambarajah 1: Hubung kait Dokumen

VIII. KATEGORI SISTEM DAN APLIKASI DI KERAJAAN NEGERI MELAKA

Beberapa aplikasi dan sistem telah dibangunkan dan digunapakai oleh Jabatan/ Agensi Kerajaan Negeri. 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	Proses Yang Disokong
1.	Rangkaian Kawasan Luas (*Wide Area Network- WAN*) dan Rangkaian Kawasan Setempat (*Local Area Network –LAN*)	Semua Jabatan	Hantaran data/ maklumat/ e-mel
2.	Portal Rasmi Kerajaan Negeri Melaka	Semua Jabatan	Penyebaran maklumat dan interaksi antara rakyat dan Kerajaan Negeri Melaka
3.	Sistem e-MMKN	Semua Jabatan	Penyediaan dan penyaluran kertas risalat Majlis Mesyuarat Kerajaan Negeri
4.	Sistem e-Tanah	Pentadbiran Tanah Negeri Melaka	Urusan berkaitan tanah dan percukaian
5.	Sistem Perakaunan dan Kewangan Standard - SPEKS	Semua Jabatan	Pentadbiran kewangan, akaun dan pembayaran secara elektronik
6.	Gerbang Pembayaran Bersepadu Kerajaan	Lembaga Perumahan,	Terimaan bayaran secara elektronik dari

Bil.	Sistem atau Aplikasi Penting dan Kritikal	Kegunaan	Proses Yang Disokong
	Negeri Melaka (e-Bayar)	Perbadanan Ketua Menteri , Jabatan Kewangan dan Perbendaharaan Negeri Melaka, Tabung Amanah Pendidikan Negeri Melaka, Majlis Perbandaran Hang Tuah Jaya, Majlis Perbandaran Jasin, Majlis Perbandaran Alor Gajah	orang awam
7.	Sistem Penganugerahan Darjah Kebesaran Negeri Melaka	Jabatan Ketua Menteri	Urusan penganugerahan dan catitan latar belakang penerima pingat
8.	E-mel dan Kalendar Rasmi Kerajaan Negeri Melaka	Semua Jabatan	E-mel dan kalendar
9.	e-TAPEM	Tabung Amanah Pendidikan Negeri Melaka	Urusan bantuan dan pinjaman pelajaran anak Negeri Melaka
10.	e-SPARA	Lembaga Perumahan Melaka, Pejabat Daerah dan Tanah	Pentadbiran akaun rumah awam/ pangsa dan pemantauan
11.	*Sistem e-Syariah*	Mahkamah Syariah Negeri Melaka	Mempertingkatkan kualiti pentadbiran Institusi Kehakiman dalam pengurusan kes mahkamah Syariah
12.	Perkhidmatan Web/ Application Hosting	Semua Jabatan	Menyediakan perkhidmatan *hosting* bagi web dan aplikasi Jabatan/ Agensi

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

IX. TANGGUNGJAWAB

Semua kakitangan Kerajaan Negeri dan pembekalpembekal yang memberi khidmat, atau bertindak selaku ejen kepada Jabatan/ Agensi masing-masing hendaklah:

- Mengambil semua langkah untuk menjaga (*safeguard*) maklumat yang wujud, terima atau kawal serta kemudahan yang mereka gunakan;
- Mematuhi Polisi dan Standard Keselamatan ICT Negeri Melaka;
- Melaporkan dengan segera semua insiden keselamatan kepada pihak pengurusan bagi memastikan tindakan yang wajar diambil; dan
- Menggunakan dengan baik aset maklumat Kerajaan Negeri 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 Polisi dan Standard yang memungkinkan tindakan disiplin.

Pelaksanaan Polisi dan Standard adalah tanggungjawab pihak Pengurusan Kerajaan Negeri dan akan dipantau oleh Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka. Manakala pelaksanaan Prosedur Keselamatan ICT Negeri Melaka adalah tanggungjawab Ketua Jabatan/ Agensi masing-masing.

X. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN

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

Bahagian Teknologi Maklumat dan Komunikasi (BTMK), Jabatan Ketua Menteri Melaka bertanggungjawab untuk mengemaskini dan memperbetulkan dokumen ini berdasarkan kelulusan Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka.

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

Nama	:	Ketua ICT Negeri, Bahagian Teknologi Maklumat dan Komunikasi
Alamat	:	Aras 1, Blok Temenggong, Seri Negeri, Hang Tuah Jaya, Ayer Keroh, 75450 Melaka
Telefon	:	+606-333 3333
Faksimili	:	+606-232 8620
E-mel	:	<pengarahict>*@melaka.gov.my

* <pengarahict> tertakluk kepada Ketua BTMK semasa

XI. 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 Negeri Melaka.
2.	Pegawai Keselamatan ICT (atau ICTSO Jabatan)	Pegawai Keselamatan ICT Jabatan bertanggungjawab ke atas keseluruhan pematuhan Polisi Keselamatan ICT Negeri Melaka. Sekiranya Jabatan memerlukan pengecualian (sementara atau tetap) dalam pematuhan Polisi Keselamatan, 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 polisi keselamatan ICT.
4.	Juru Audit Jabatan	Kakitangan Jabatan/ Agensi yang ditugaskan untuk menjalankan audit pemantauan dalam Jabatan/ Agensi 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 polisi keselamatan ICT.
6.	Jawatankuasa Pemandu Teknologi	Jawatankuasa ini menentukan hala tuju pelaksanaan ICT Negeri Melaka, menetapkan polisi keselamatan ICT dan memantau tahap pelaksanaan serta

Bil.	Nama Peranan	Keterangan Bidang Tugas
	Maklumat Negeri Melaka	pematuhan polisi oleh semua kakitangan Kerajaan Negeri Melaka.
7.	Ketua Jabatan/ Agensi atau Pegawai Pengawal	Pegawai yang menyokong atau mengesahkan permohonan ID dan hak capaian pengguna dalam Jabatan/ Agensi 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/ Agensi sendiri dalam penyelesaian masalah atau insiden dalam Jabatan/ Agensi.
9.	Khidmat Bantuan Tahap 2	Bantuan daripada pihak yang membekalkan aplikasi atau sistem dibawah pengurusan Pemilik Aplikasi atau Sistem.
10.	Pemilik Aset	Ketua Jabatan/ Agensi 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.
14.	Pengguna-	Pegawai/ kakitangan yang menggunakan aplikasi atau

Bil.	Nama Peranan	Keterangan Bidang Tugas
	Pengguna	sistem bagi urusan rasmi.
15.	Pengurus Aplikasi/ Sistem	Pegawai yang bertanggungjawab terhadap aplikasi atau sistem yang dibangunkan dalam Jabatan/ Agensi atau dimiliki oleh Jabatan/ Agensi. 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.
17.	Pentadbir Pangkalan Data	Pentadbir Pangkalan Data bertanggungjawab memastikan pangkalan data berfungsi dengan baik dan dikemaskini dari semasa ke semasa.
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.	Penyelaras Prosedur	Pegawai yang bertanggungjawab mengemaskini dan menyebarkan prosedur-prosedur berkaitan kegunaan, pengurusan dan penyelenggaraan aplikasi atau perkhidmatan sokongan.

Jadual 2: Terminologi Fungsi/ Peranan dan Bidang Tugas

XII. DEFINISI POLISI, STANDARD DAN PROSEDUR

1. Polisi

Polisi adalah kenyataan atau arahan yang menerangkan keperluan setiap domain ICT. Kenyataan polisi adalah ringkas dan padat supaya senang difahami, diingati dan dipatuhi oleh semua yang berkaitan.

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.

3. Prosedur

Prosedur adalah langkah-langkah yang khusus dan tepat bagaimana sesuatu polisi atau standard mesti dilaksanakan. Ini termasuk langkah-langkah yang lebih terperinci (*detailed steps*), borang yang perlu diguna, jadual semakan, aliran proses (*process or workflow*) dan lain-lain.

XIII. POLISI KESELAMATAN ICT NEGERI MELAKA

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. Walaubagaimanapun, 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.

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 mengikut pembahagian tanggungjawab, bidang kuasa dan hubungkait.

2.2. Pernyataan Polisi

Semua kakitangan yang mengguna, mentadbir atau mengurus aplikasi dan sistem di Jabatan/ Agensi 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

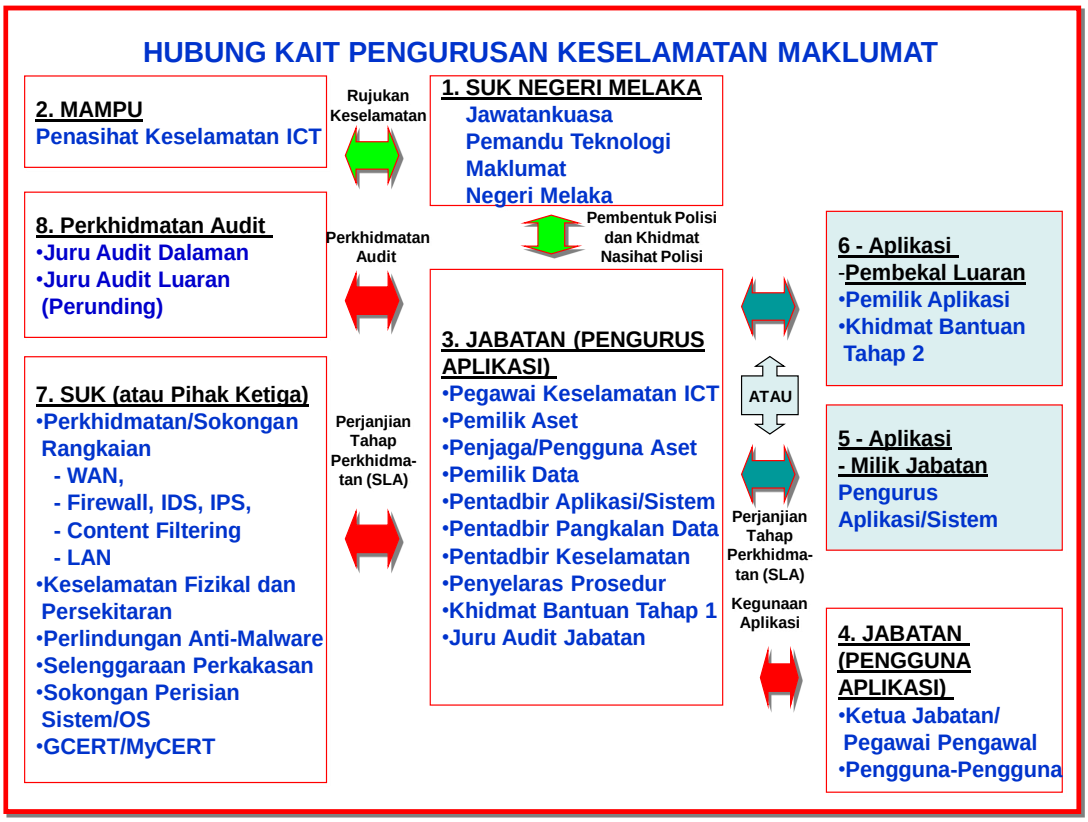
Pengurusan Keselamatan Maklumat dilaksanakan dengan mewujudkan fungsi-fungsi tertentu dengan tanggungjawab tersendiri. Fungsi-fungsi ini perlu bekerjasama dan berhubung kait antara satu sama lain untuk memastikan bahawa keseluruhan objektif keselamatan maklumat tercapai.

Setiap Jabatan/ Agensi 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. Hubung kait Pengurusan Maklumat

Hubung kait antara semua yang terlibat di dalam mengurus, mentadbir, menyelenggara, memberi perkhidmatan sokongan, mengguna aplikasi

atau sistem adalah seperti dalam Rajah 1:



Rajah 1 : Hubung kait Pengurusan Keselamatan Maklumat

Penerangan ringkas berkaitan Rajah 1 adalah seperti berikut :

1 : SUK Negeri Melaka

Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka dipengerusikan oleh YB. Setiausaha Kerajaan Negeri dan dianggotai oleh Ketua Jabatan/ Agensi Negeri, dan berkewajipan menentukan polisi keselamatan dan memantau tahap pelaksanaan dan pematuhan dasar.

2 : MAMPU

MAMPU memberi khidmat nasihat dan panduan berkaitan hal-hal keselamatan ICT secara keseluruhan untuk semua Jabatan Kerajaan Pusat atau Kerajaan Negeri.

3 : Jabatan/ Agensi (Pengurus Aplikasi)

Jabatan/ Agensi yang mempunyai aplikasi dan sistem bertanggungjawab mengurus dan menguatkuasakan pentadbiran keselamatan dan khidmat bantuan terhadap aplikasi tersebut.

Sebuah Jabatan/ Agensi boleh menguruskan lebih dari satu (1) aplikasi dan sistem. Aplikasi tersebut boleh digunakan oleh pengguna dalaman atau di Jabatan/ Agensi lain.

Untuk aplikasi dan sistem dalam Kategori 1, fungsi Pentadbir Aplikasi/ Sistem, Pentadbir Pangkalan Data dan Pentadbir Keselamatan mesti diasingkan, kecuali sekiranya rekabentuk aplikasi sedia ada tidak memperuntukkan keperluan berasingan atau tidak memerlukan pengasingan. Walau bagaimanapun, mereka yang bertanggungjawab terhadap fungsi tersebut boleh menjadi pentadbir gantian (*backup administrator*) fungsi lain apabila pentadbir utama bercuti atau berkhusus. Kegunaan logon ID yang berasingan perlu dikawal supaya jejak guna ID (*audit trail of use of ID*) boleh dikenalpasti.

4 : Jabatan/ Agensi (Pengguna Aplikasi)

Pengguna-pengguna apliksai dan sistem yang ditadbirkan oleh Jabatan/ Agensi sendiri atau Jabatan/ Agensi lain.

5 : Aplikasi (Milik Jabatan/ Agensi)

Jabatan membangunkan aplikasi khusus untuk kegunaan sendiri dan/ atau membekalkannya untuk kegunaan jabatan lain.

6 : Aplikasi (Pembekal Luaran)

Jabatan menggunakan aplikasi yang dibangunkan dan dimiliki oleh Jabatan/ Agensi lain. Contoh aplikasi ialah Sistem e-Tanah dari Kementerian Sumber Asli dan Alam Sekitar. Khidmat meja bantuan tahap

2 juga dikendalikan oleh Jabatan yang membekalkan aplikasi tersebut. **Untuk aplikasi dalam Kategori 1, Perjanjian Tahap Perkhidmatan atau SLA mesti wujud antara pembekal aplikasi dan Jabatan yang mengurus aplikasi sama ada secara terus atau melalui wakil Jabatan berkenaan (misalnya Bahagian Teknologi Maklumat dan Komunikasi) dalam Kerajaan Negeri Melaka.**

7 : Setiausaha Kerajaan Negeri (SUK) atau PembekalPembekal (Pihak ketiga)

Semua perkhidmatan sokongan termasuk kegunaan WAN, *firewal*l, *Intrusion Detection Systems* (IDS), *Intrusion Protection Systems* (IPS), *Content Filtering* dan LAN, keselamatan fizikal, selenggaraan perkakasan dan sistem pengoperasian yang tidak ditadbirkan oleh Jabatan/ Agensi sendiri, yang mana perkhidmatan diberi oleh SUK atau pihak ketiga.

Untuk aplikasi Kategori 1, Perjanjian Tahap Perkhidmatan atau SLA hendaklah diwujudkan:

a. **Di antara Jabatan/ Agensi yang mengurus aplikasi dan penyedia perkhidmatan terus dari SUK - Bahagian Teknologi Maklumat dan Komunikasi. Contoh perkhidmatan ialah selenggaraan Pusat Data di Seri Negeri dan LAN di Seri Negeri;**

b. **Di antara Jabatan/ Agensi yang mengurus aplikasi dan pemberi perkhidmatan menerusi SUK - Bahagian Teknologi Maklumat dan Komunikasi. Contoh perkhidmatan sokongan rangkaian WAN; dan**

c. **Di antara Jabatan yang mengurus aplikasi dan pemberi perkhidmatan pihak ketiga secara terus menerus. Ini biasa didapati di PTG dan PTD dan lain-lain Jabatan di luar Seri Negeri. Contoh perkhidmatan mungkin termasuk selenggaraan LAN, penghawa dingin Pusat Data , UPS dan pelayan, bergantung kepada keperluan khusus Jabatan berkenaan.**

Untuk menangani serangan virus, *malware* dan ancaman lain,

a. *Government Computer Emergency Response Team* (GCERT) perlu dimaklumkan walaupun perkhidmatan GCERT mungkin tidak perlu. Syarat-syarat perkhidmatan antara GCERT dan Agensi-Agensi Kerajaan yang sedia ada perlu di patuhi; dan

b. *Malaysian Computer Emergency Response Team* (MyCERT) tidak wajib dimaklumkan melainkan perkhidmatan khusus dari MyCERT, contohnya penyiasatan forensik diperlukan jika berlaku pencerobohan aplikasi. Syarat-syarat perkhidmatan yang ditentukan oleh MyCERT yang sedia ada perlu diambilkira.

<u>8: Perkhidmatan Audit</u>

Perkhidmatan audit dalaman diselaraskan oleh Jabatan/ Agensi manakala audit luaran dilakukan oleh pakar atau perunding yang berkebolehan melakukan audit teknikal terhadap sistem dan proses pengurusan keselamatan ICT.

2.5. Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka

a. Dipengerusikan oleh YB. Setiausaha Kerajaan Negeri dan dianggotai oleh Ketua Jabatan/ Agensi negeri;

b. Menentukan hala tuju pelaksanaan ICT Negeri Melaka, menetapkan polisi keselamatan dan memantau tahap pelaksanaan serta pematuhan polisi oleh semua kakitangan Kerajaan Negeri Melaka; dan

c. Memberi arahan dari masa ke semasa kepada semua Jabatan/ Agensi untuk memantapkan fahaman dan amalan keselamatan maklumat.

2.6. Ketua Pegawai Maklumat

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

a. Memastikan Pelan Strategik ICT (PSICT) Jabatan/ Agensi selari dengan PSICT Sektor Awam dan Pelan Strategik Jabatan/ Agensi;

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/ Agensi.

2.7. Pegawai Keselamatan ICT

Pegawai Keselamatan ICT mesti wujud di setiap Jabatan/ Agensi. Beliau juga dikenali sebagai *ICT Security Officer* (ICTSO Jabatan). Tanggungjawab ICTSO adalah seperti berikut:

a. Memastikan Jabatan/ Agensi mematuhi Polisi dan Standard Keselamatan ICT Negeri Melaka;

b. Bekerjasama dengan ICTSO Kerajaan Negeri Melaka dalam menyelaras dan memberi maklumbalas berkaitan pelaksanaan keselamatan maklumat di Jabatan masing- masing; dan

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

2.8. Pemilik Aset

Pemilik Aset adalah Ketua Jabatan/ Agensi atau Pegawai Pengawal yang bertanggungjawab terhadap pemilikan aset bagi pihak Kerajaan Negeri. 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. Contoh Pemilik Aplikasi/ Sistem ialah Kementerian Sumber Asli yang membekalkan dan memberi Khidmat Bantuan Tahap 2 terhadap aplikasi e-Tanah.

Tanggungjawab Pemilik Aplikasi/ Sistem adalah seperti berikut:

a. Membekalkan sistem yang mematuhi aspek-aspek keselamatan mengikut garis panduan Kerajaan dan piawaian antarabangsa seperti ISO 27002, *Code of Practice for Information Security*, 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. Memberi khidmat sokongan Tahap 2 kepada Jabatan/ Agensi; dan

e. 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/ Agensi 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 piawaian antarabangsa seperti ISO 27002, *Code of Practice for Information Security*, 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. Memberi khidmat sokongan Tahap 1 kepada pengguna-pengguna aplikasi atau sistem; dan

e. 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/ Agensi 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. Penyelaras Prosedur

Penyelaras Prosedur bertanggungjawab menyelaras proses kemaskini semua prosedur dari semasa ke semasa. Di antara tugas beliau adalah:

a. Menyimpan senarai penerima dokumen prosedur supaya pengagihan prosedur yang terkini dapat dikawal;

b. Mempastikan prosedur yang dikemaskini dicetak dan disalin untuk diagihkan kepada semua yang berkaitan; dan

c. Mengatur atau memberi arahan kepada penerima prosedur untuk melupuskan bahagian dokumen prosedur lama yang tidak digunapakai lagi.

2.17. Ketua Jabatan/ Agensi atau Pegawai Pengawal

Ketua Jabatan/ Agensi 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/ Agensi 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.

2.18. Pengguna-Pengguna

Pengguna-pengguna bertanggungjawab seperti berikut:

a. Memahami Polisi dan Standard 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/ Agensi 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 BTMK supaya tindakan dapat diambil untuk diselesaikan.

f. Menandatangani Surat Akuan Pematuhan Polisi dan Standard Keselamatan ICT Negeri Melaka seperti di Lampiran 1.

2.19. Khidmat Bantuan Tahap 1

Pengurus Aplikasi atau Pemilik Data hendaklah mewujudkan fungsi Khidmat Bantuan Tahap 1 (*Helpdesk with first level support*) untuk memberi bantuan kepada Pengguna yang menghadapi masalah penggunaan aplikasi.

Di antara Tugas Khidmat Bantuan Tahap 1 adalah:

a. Menyalurkan semua laporan insiden atau masalah kepada pegawai yang bertanggungjawab;

b. Membantu pengurusan ICT dalam pemantauan bagi laporan yang belum diselesaikan dan mengambil tindakan susulan sebagaimana diarahkan oleh pengurusan ICT;

c. Memajukan laporan insiden atau masalah kepada fungsi Khidmat Bantuan Tahap 2, sekiranya aplikasi dibekalkan dan diselenggarakan oleh pihak ketiga; dan

d. Mengkaji corak (*trend)* laporan insiden dan merangka penyelesaian jangka panjang supaya insiden yang kerap berlaku dapat dikawal atau dikurangkan.

2.20. Khidmat Bantuan Tahap 2

Khidmat Bantuan Tahap 2 (*Helpdesk with second level support*) adalah untuk memberi bantuan kepada fungsi Khidmat Bantuan Tahap 1 sekiranya mereka tidak dapat mengatasi masalah yang dilaporkan. Khidmat Bantuan Tahap 2 dikendalikan oleh pihak ketiga (pembekal) yang membekalkan dan menyelenggara aplikasi berkaitan Perjanjian Tahap Perkhidmatan atau SLA hendaklah diwujudkan dengan pembekalpembekal tersebut bagi memberi perkhidmatan bantuan yang diperlulan.

Diantara tugasan Khidmat Bantuan Tahap 2 adalah:

a. Menyelesaikan masalah mengikut tahap kritikal insiden atau laporan;

b. Merakam semua laporan insiden atau masalah;

c. Memantau senarai laporan yang belum diselesaikan dan mengambil tindakan penyelesaian; dan

d. Mengkaji corak (*trend)* laporan insiden dan merangka penyelesaian jangka panjang supaya insiden yang kerap berlaku dapat dikawal atau dikurangkan.

2.21. Juru Audit Jabatan/ Agensi

Juru Audit Jabatan/ Agensi bertanggungjawab melaksanakan audit pemantauan terhadap sistem dan proses pengurusan keselamatan ICT.

Pengauditan tidak perlu dilakukan serentak untuk semua bahagian ICT pada satu-satu masa. Ia boleh dilakukan oleh kakitangan berlainan bahagian dalam satu Jabatan/ Agensi. Contoh: Kakitangan yang bertugas menyelenggarakan rangkaian boleh mengaudit bahagian keselamatan hak capaian aplikasi atau pentadbiran aplikasi dan sebaliknya. Kakitangan itu tidak dibenarkan mengaudit bidang tugasnya sendiri, selaras dengan keperluan pengasingan kerja.

2.22. Juru Audit Dalaman

Juru Audit Dalaman bertanggungjawab mengaudit sistem dan proses pengurusan keselamatan ICT di seluruh Jabatan/ Agensi dan mencadangkan langkah-langkah pembetulan.

2.23. Juru Audit Luaran

Juru Audit Luaran bertanggungjawab mengaudit sistem dan proses pengurusan keselamatan ICT di Jabatan dan melaporkan teguran-teguran jika terdapat ketidakpatuhan. Oleh kerana kepakaran teknikal khusus diperlukan, maka pakar atau perunding luar dilantik bagi menjalankan audit luaran.

Seksyen 3. Pengurusan Aset Berkaitan Maklumat

3.1. Tujuan dan Skop

Tujuan Polisi Pengurusan Aset Berkaitan Maklumat adalah 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 penghawa dingin, *centralised uninterruptible power supply* dansistem 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*);

   i. Penjaga Aset atau Pengguna Aset (*asset custodian*);

   ii. Klasifikasi aset (untuk aset maklumat atau data);

   iii. Lokasi aset;

   iv. Jangkahayat aset (sekiranya maklumat ini ada);

   v. Harga perolehan aset (sekiranya maklumat ini ada);

vi. Hubung kait aset dengan aset lain (sekiranya maklumat hubung kait aset kurang jelas fungsinya); dan

vii. Penyelenggara aset (*asset maintainer*).

b. Aset maklumat dalam bentuk digital atau *hardcopy* perlu diklasifikasikan berdasarkan tahap kritikal atau kepentingan (*criticality or importance*) supaya langkah perlindungan dan pengurusan yang sewajarnya dapat diaturkan;

c. Pemilik aset maklumat bertanggungjawab mengklasifikasikan maklumat dan menyemak klasifikasi dari semasa ke semasa;

d. Aset maklumat perlu ditandakan mengikut klasifikasi yang ditentukan dengan sewajarnya;

e. Aset maklumat berperingkat perlu dimaklumkan kepada semua pengguna yang mengendalikan atau mentadbirkan aset berkaitan supaya kawalseliaan dan pengendalian yang sewajarnya dapat dipatuhi dan dikuatkuasakan; dan

f. Pelupusan aset hendaklah mengikut garis panduan Kerajaan. Khususnya data pada cakera keras, cakera padat (CD atau DVD), cakera liut dan *media backup* yang lain mesti dikosongkan atau dimusnahkan supaya data tidak dapat diekstrak (*extract*) oleh pihak yang tidak bertanggungjawab.

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.

4.2. Pernyataan Polisi

Semua kakitangan Jabatan/ Agensi 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/pembekaljuga hendaklah mematuhi Polisi Keselamatan ICT.

4.3. Standard 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.

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;

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.

4.3.4. Kewajipan 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 memperakui kefahaman mereka terhadap:

- Tanggungjawab dalam memastikan kerahsiaan maklumat;
- Tanggungjawab untuk melaporkan pelanggaran polisi atau ketidakpatuhan terhadap keselamatan pengendalian

maklumat atau keselamatan fizikal, walaupun belum terbukti kesilapan tersebut; dan

- Kesedaran bahawa tindakan disiplin boleh diambil terhadap mereka sekiranya tidak mematuhi polisi keselamatan.

4.3.5. Pengendalian Kakitangan Yang Berpindah Atau Bersara

a. Ketua Jabatan/ Agensi hendaklah memaklumkan kepada Pengurus Sistem sekiranya terdapat kakitangan dibawah jagaannya berpindah atau bersara;

b. Kata laluan bagi pengguna berkenaan hendaklah diubah selepas tarikh perpindahan atau persaraan kakitangan berkenaan dan Logon IDnya digantung dalam tempoh tiga bulan sebelum dimansuhkan;

c. Ketua Jabatan hendaklah memastikan penyerahan tugas terutama sekali dalam tanggungjawab pengendalian maklumat dilaksanakan kepada pengganti pegawai berkenaan; dan

d. 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.

4.3.6. 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. Kakitangan perlu memberi kerjasama sepenuhnya untuk membantu penyiasatan dan penyelesaian masalah atau insiden yang dihadapi.

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.

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 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, Pusat Datadan penjana kuasa kecemasan;

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; dan

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.

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.

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 (*logging*) 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.

Penggunaan komputer untuk tugas rasmi hendaklah dirangkaikan ke rangkaian Melaka*Net dan sambungan ke rangkaian lain adalah tidak dibenarkan sama sekali.

Penggunaan rangkaian tanpa wayar *Wireless)* yang disediakan di Jabatan Kerajaan Negeri Melaka adalah untuk kegunaan orang awam dan perkakasan mudah alih kakitangan. Manakala penggunaan rangkaian tanpa wayar (*Wireless LAN*) adalah tidak dibenarkan kecuali dengan kelulusan dan mesti mematuhi syarat-syarat yang ditetapkan oleh Pegawai Keselamatan ICT Kerajaan Negeri ICTSO.

6.3. Standard 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 Rangkaian

a. Pengurusan konfigurasi rangkaian adalah untuk memantapkan prestasi dan keselamatan sistem. Pengurusan tersebut tidak melibatkan perkakasan tetapi melibatkan konfigurasi seperti berikut:
   i. Polisi firewall atau IDS atau IPS; dan
   ii. Alamat IP rangkaian dan pengasingan LAN (*LAN segments*).

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 (*troubleshooting and rectification*).

c. Rekod perubahan konfigurasi (sebelum dan selepas perubahan) hendaklah diarkibkan;

d. Semua perubahan besar hendaklah mendapat kelulusan pemilik, manakala perubahan biasa hanya perlu mendapat kelulusan Penjaga Aset;

e. 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.

6.3.1.3. 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. Penjaga Aset hendaklah menentukan bahawa semua perubahan sementara dilaksanakan dalam tempoh yang diluluskan dan semua konfigurasi diubah ke konfigurasi asal sebelum tamat tempoh; dan

c. **Untuk perubahan sementara yang melibatkan sistem atau aplikasi dalam Kategori 1**;
   i. Semua aktiviti kerja perubahan perlu dicatitkan oleh pelaksana perubahan untuk disemak oleh Penjaga Aset selepas perubahan dilaksanakan; dan
   ii. Pemilik Data aplikasi atau sistem yang terlibat perlu dimaklumkan berkaitan perubahan sementara tersebut.

6.3.1.4. 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 perkhidmatan diteruskan atau melaksanakan urusan penting;

b. Perubahan dalam keadaan kecemasan boleh dilakukan oleh Penjaga Aset*;*

c. **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;**

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

e. Pemilik Aset hendaklah memantau kekerapan perubahan dalam keadaan kecemasan dan merangka tindakan jangka panjang untuk mengurangkan perubahan.

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; dan.

b. Pastikan bahawa semua aktiviti penting yang menggunakan ID berkenaan dijejak melalui *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*). ID hak capaian tinggi tidak boleh digunakan untuk tugas, pemantauan dan senggaraan harian; dan

c. Kegunaan ID hak capaian tinggi hendaklah dicatitkan untuk semakan dari masa ke semasa.

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. 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.

6.3.5. Senggaraan 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.

6.3.6. Perjanjian Tahap Perkhidmatan

a. Pastikan bahawa wujudnya Perjanjian Tahap Perkhidmatan terutama sekali dengan pembekal perkhidmatan luar seperti

Telekom Malaysia 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.

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; dan

e. *Backup* perlu dilakukan apabila:

i. Aplikasi atau sistem berubah atau naiktaraf; dan

ii. Pangkalan data atau fail berubah.

f. Kekerapan aktiviti *backup* bergantung kepada pentingnya aplikasi atau sistem. **Untuk Kategori 1, *backup* penuh data (*full data backup*) perlu dilakukan seminggu sekali manakala backup data tambahan atau perubahan (*incremental or differential backup*) perlu dilakukan setiap hari.**

6.3.8. Komputer Kerajaan Negeri

Komputer yang dipasang di premis Kerajaan Negeri dan Jabatan-jabatan disambung kepada rangkaian yang ditadbirkan oleh BTMK. Perubahan atau tambahan sambungan ke rangkaian lain dilarang dilakukan oleh pengguna melainkan atas kebenaran kakitangan selenggaraan BTMK.

6.3.9. Rangkaian Tanpa Wayar

Penggunaan rangkaian tanpa wayar hanya dibenarkan kepada pelawat dan orang awam yang datang berurusan bagi rangkaian tanpa wayar *(Open Wireless)* dan pengguna rangkaian tanpa wayar *(Wireless LAN)* yang telah diluluskan oleh Pegawai Keselamatan ICT Kerajaan Negeri. Pemohon hendaklah mengemukakan alasan yang munasabah untuk keperluan tersebut. Pegawai Keselamatan ICT Kerajaan Negeri hendaklah mengkaji permohonan tersebut dan menggariskan syarat-syarat tertentu untuk dipatuhi oleh pemohon.

Pemohon hendaklah memperakui pematuhan syarat-syarat yang digariskan sebelum kegunaan peralatan rangkaian tanpa wayar dibenarkan.

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 Jabatan / Agensi.

6.3.11. 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.

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.

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 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; dan

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.

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.

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/ Agensi perlu menyediakan senarai terkini pengguna aplikasi atau sistem sekurang-kurangnya setahun sekali;

d. Pentadbir Keselamatan perlu menyemak dan menyelaras senarai terkini pengguna dan membandingkannya dengan borang permohonan dan pelupusan ID sekurang-kurangnya setahun sekali; dan

e. 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; dan

b. 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 2008.

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 2008. 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. Hak capaian sementara dalam keadaan kecemasan (*emergency*) dan utiliti berkuasa (*powerful utilities*) hendaklah dikawal dan dipantau kegunaannya.

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.

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 Pembangunan dan Penyelenggaraan Aplikasi

8.3.1. 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. 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;

c. Aplikasi hendaklah berupaya menjana *audit trails* bagi transaksi penting dalam aktiviti:
   i. Kemasukan data;
   ii. Perubahan data; dan
   iii. Penghapusan data.

d. 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*).

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

8.3.2. 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;
   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;
   vi. Proses ujian aplikasi dilakukan dengan sempurna dan menyeluruh;

vii. Latihan pengguna disediakan; dan

viii. 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/ Agensi.

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 Pengurusan Insiden

9.3.1. Laporan Insiden dan Penyelesaian

a. Setiap insiden hendaklah dilaporkan. Insiden yang dilaporkan secara lisan atau emel perlu disusuli dengan borang laporan insiden yang lengkap;

b. Meja bantuan hendaklah mengagihkan setiap insiden kepada kakitangan bantuan yang bertugas untuk penyelesaian mengikut prioriti;

c. Kakitangan bantuan yang bertugas perlu merangka tindakan pembetulan yang sesuai untuk menyelesaikan masalah atau insiden;

d. Semua yang terlibat hendaklah bekerjasama dan berhubung rapat untuk menyelesaikan insiden tersebut; dan

e. Sekiranya penyelesaian insiden adalah di luar bidang tugas kakitangan bantuan, maka laporan insiden tersebut hendaklah dimajukan ke peringkat lebih tinggi (sama ada di dalam Kerajaan Negeri atau pihak luar).

9.3.2. Pemantauan Penyelesaian Laporan Insiden

a. Semua laporan perlu dipantau tahap atau peringkat penyelesaiannya dan tindakan susulan perlu diambil untuk menyelesaikan inisiden yang serius secepat mungkin; dan

b. Kajian perlu dilakukan dari semasa ke semasa untuk mengenalpasti corak laporan insiden dan merangka penyelesaian jangka panjang supaya insiden yang kerap berlaku dapat dikawal atau dikurangkan.

Seksyen 10. Pengurusan Kesinambungan Perkhidmatan

10.1. Tujuan dan Skop

'Pengurusan Kesinambungan Perkhidmatan' menyediakan kerangka pengurusan (*management framework*) untuk memulihkan perkhidmatan secara formal supaya Jabatan/ Agensi dapat meneruskan operasi sekiranya berlaku gangguan ICT yang berpanjangan.

Polisi ini dikuatkuasakan ke atas semua sistem dalam **Kategori 1** di bawah kawalan Jabatan/ Agensi 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 Pengurusan Kesinambungan Perkhidmatan

10.3.1. Kewajipan Merangka Kesinambungan Perkhidmatan

a. Pihak pengurusan hendaklah mewujudkan satu (1) jawatan kuasa khusus untuk merancang dan membangunkan Pelan Kesinambungan Perkhidmatan (PKP). Tugas dan tanggungjawab jawatankuasa tersebut hendaklah dikenalpasti dan dipersetujui.

10.3.2. Analisa Dan Mengenalpasti Perkhidmatan Kritikal

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

b. Metodologi tersebut hendaklah mengenalpasti Analisis Impak Perkhidmatan (*Business Impact Analysis*) dan Anggaran Penilaian Risiko (*Risk Evaluation Assessment*) akibat kelemahan dan ancaman bagi membangunkan Strategi Pemulihan (*Recovery Strategies*).

10.3.3. Perlaksanaan Pelan dan Ujian

a. Pelan kesinambungan perkhidmatan perlu dirangka dan diuji kesesuaian dan ketepatannya dari semasa ke semasa;
b. Dokumen pelan kesinambungan perkhidmatan perlu dikemas kini dari semasa ke semasa dan diedarkan kepada semua yang berkaitan; dan
c. Semua yang berkaitan hendaklah dilatih untuk melaksanakan bidang tugas masing-masing apabila berlaku gangguan perkhidmatan yang memerlukan pelan kesinambungan perkhidmatan diaktifkan.

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/ Agensi.

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 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.

11.3.2. Semakan Polisi dan Standard Dan Pematuhan

a. Polisi dan Standard hendaklah disemak dan dikemaskini dari masa ke semasa untuk menentukan ia menepati keperluan kini dan akan datang; dan

b. Semua Ketua Jabatan/ Agensi hendaklah memastikan bahawa Polisi dan Standard dipatuhi oleh kakitangan dalam semua Jabatan/ Agensi.

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/ Agensi.

11.3.4. Hak Capaian Untuk Juru Audit

a. Setelah digunakan dalam tempoh audit, hak capaian sementara tersebut perlu dimansuhkan.

   Hak capaian sementara boleh diberi kepada Juru Audit, sekiranya terdapat keperluan.

LAMPIRAN 1

BORANG AKUAN PEMATUHAN
POLISI DAN STANDARD KESELAMATAN ICT NEGERI MELAKA

Nama : ……

No. Kad Pengenalan : ……

Jawatan : ……

Jabatan / Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi dan Standard Keselamatan ICT Negeri Melaka; dan

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

Tandatangan: …….

Tarikh : …….

Pengesahan Ketua Pegawai Maklumat / Pegawai Keselamatan ICT

……..
(Nama)

b.p Setiausaha Kerajaan Negeri Melaka

Tarikh : ……

BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
JABATAN KETUA MENTERI MELAKA