DASAR
KESELAMATAN ICT
NEGERI MELAKA

VERSI 2.5

DASAR KESELAMATAN ICT (DKICT) NEGERI MELAKA

“MELAKAKU MAJU JAYA, RAKYAT BAHAGIA MENGGAMIT DUNIA”

“BIJAK LAKSANA TUAH, BERANI LAKSANA JEBAT”

“MALAYSIA MADANI”

“BERKHIDMAT UNTUK NEGARA”

Tidak dibenarkan mengeluar ulang mana-mana bahagian artikel, ilustrasi dan isi kandungan buku ini dalam apa juga bentuk dan dengan apa cara juga sama ada secara elektronik, fotokopi, mekanik, rakaman atau cara lain sebelum mendapat izin bertulis daripada penerbit.

Diterbitkan Oleh :
Jabatan Ketua Menteri Melaka
Bahagian Teknologi Maklumat dan Komunikasi
Aras 1, Blok Temenggong, Seri Negeri, Hang Tuah Jaya,
75450, Ayer Keroh, Melaka.

KANDUNGAN

PENGENALAN DOKUMEN

NAMA DOKUMEN	**:**	**Dasar Keselamatan ICT Negeri Melaka**
VERSI	**:**	**2.5**
TARIKH	**:**	**8 April 2024**

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 Maklumat	Pindaan Pusat Data di para 3.1

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		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 • Tambahan perenggan di para 2.3: Manakala maklumat milik kerajaan perlu disimpan di premis milik

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			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 Persekitaran	• Pembetulan ejaan mempamirkan kepada mempamerkan

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			• 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 • Pembetulan frasa di para 6.2 • Pembetulan frasa di para 6.3.9

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			• 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
6.	17 Mei 2017	Keseluruhan Dokumen	• Perubahan major bagi penggabungan dengan dokumen Prosedur Keselamatan ICT Negeri Melaka • Perubahan nama dokumen kepada Dasar Keselamatan ICT Negeri Melaka
7	3 Disember 2018	Kandungan	• Tambahan perenggan 2.9 Pegawai Keselamatan Jabatan (CGSO)
		VI. DOKUMEN RUJUKAN	• tambah Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		X. PENERANGAN TERMINOLOGI FUNGSI	• tambahan peranan Pegawai Keselamatan Jabatan (CGSO)
		Seksyen 2. Pengurusan Keselamatan Maklumat	• Pindaan perenggan 2.8. Pegawai Keselamatan ICT • Tambahan perenggan 2.9 Pegawai Keselamatan Jabatan (CGSO) • Pindaan Item 2.19. Pengguna-Pengguna
		Seksyen 3. Pengurusan Aset Berkaitan Maklumat	• Pembetulan frasa di para 3.1.b dan 3.4.a • Pindaan Item 3.4 (b)
		Seksyen 6. Pengurusan Operasi dan Rangkaian	• Pindaan diperenggan 6.3.1.2, 6.3.1.3, 6.3.1.4, 6.3.1.5, 6.3.3, 6.3.7 dan 6.3.11, • Tambahan perenggan baru 6.3.14. Penggunaan Peranti Peribadi
		Seksyen 7. Kawalan Capaian Logikal	• Tambahan perenggan baru 7.3.6. Kriptografi
		Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi	• Tambahan item l dan m di perenggan 8.3.2
		Seksyen 9. Pengurusan Insiden	• Pindaan di perenggan 9.3.1 • Tambahan item di perenggan 9.3.2.
		Seksyen 10. Pengurusan Kesinambungan Perkhidmatan	• Pindaan di perenggan 10.3.3
		Borang J : Penamatan Akaun Aplikasi Dan Pemulangan Peralatan ICT	• Pindaan kepada jadual

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
8.	11 Mac 2021	V. Skop Dasar Keselamatan ICT Negeri	• Pindaan Para 1 skop DKICT merangkumi pengurusan, pengendalian dan penyelenggaraan aset ICT yang terdiri daripada perkakasan, perisian, perkhidmatan, data/ maklumat dan manusia.
		VI.Penilaian Risiko Keselamatan ICT	• Penambahan Tajuk Baharu
		VIII. Kategori Sistem dan Aplikasi di Kerajaan Negeri Melaka	• Pindaan Jadual 1 : Sistem atau Aplikasi Penting dan Kritikal - Kategori 1:- i) Penambahan Agensi yang menggunakan e-bayar. ii) Penambahan item no 12: Electronic Registration and Result System (eRS) iii) Penambahan item no 13: Sistem Tender Online Melaka (STOM)
		IX. Pengemaskinian dan Penyenggaraan Dokumen	• Pindaan emel <pengarahict> kepada <ketuaict>
		X. Penerangan Terminologi Fungsi	• Pindaan Jadual 2 i) Khidmat Bantuan Tahap 1: Bantuan dari Pemilik Aplikasi/Sistem dalam penyelesaian masalah atau insiden. ii) Khidmat Bantuan Tahap 2: Bantuan daripada pihak yang membekalkan aplikasi/ sistem. iii) Pemilik Aplikasi/ Sistem: Pemilik Aplikasi/ Sistem adalah pembekal aplikasi/ sistem tersebut. Pemilik bertanggungjawab atas semua

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			pembetulan fungsi dan naiktaraf aplikasi/ sistem. iv) Pengguna Aset : Kakitangan yang bertanggungjawab terhadap keselamatan aset untuk kegunaan harian. v) Pemilik Data:Pegawai Jabatan/ Agensi yang berkepentingan terhadap kerahsiaan dan kesahihan data yang disimpan vi) v) Pengguna: Pegawai/ kakitangan yang menggunakan aplikasi/ sistem dan aset bagi urusan rasmi. vi) Pengurus Aplikasi/ Sistem: Pegawai yang bertanggungjawab terhadap pembangunan, naik taraf dan pembetulan aplikasi/ sistem. v) Pentadbir Aplikasi/ Sistem: Pentadbir Pangkalan Data adalah Fungsi teknikal yang bertanggungjawab i) memastikan pangkalan data berfungsi dengan baik dan dikemaskini dari semasa ke semasa, ii) melaksanakan perubahan pangkalan data mengikut keperluan, dan menjana dan mengemaskini log.
		Seksyen 2: Pengurusan Keselamatan Maklumat	• Pindaan tajuk para 2.15: Pentadbir Aplikasi/ Sistem/ Aset ICT • Pindaan para 2.15(c)

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			Melaksanakan instalasi *patches* dan naik taraf (*upgrade*) • Pindaan para 2.15(d) Menjana dan mengemaskini log • Penambahan di para 2.15 • 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; • Menyiasat cubaan capaian yang gagal dan mencurigakan (*suspicious failed login attempts*) serta mengambil tindakan sewajarnya, jika perlu; • Melaksanakan perubahan konfigurasi pangkalan data sekiranya diminta oleh pembekal sistem; • Menjana log akses dan perubahan data jika perlu, dan membersihkan log dari semasa ke semasa; • Melakukan *tuning* termasuk *reindexing* apabila diperlukan; dan • Memberi hak capaian pangkalan data untuk aplikasi (dan bukan kepada pengguna) dan fungsi bagi *backup* dan pemulihan (*recovery*)Pindaan Rajah (2)
		Seksyen 3: Pengurusan Aset Berkaitan Maklumat	• Pindaan para 3.4(c) Proses merekod aset menggunakan kad daftar harta modal (KEW.PA-3) atau Borang A ditunjukkan dalam Rajah 3.
		Seksyen 6. Pengurusan Operasi dan Rangkaian	• Pindaan para 6.3.1.1(b) (iv)

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			Tatacara kembali kepada konfigurasi asal sekiranya berlaku masalah semasa perubahan atau setelah perubahan dilakukan. • Item para 6.3.1.1(b) (v) dipadam • Penambahan para 6.3.15
		Seksyen 7. Kawalan Capaian Logikal	• Pindaan Rajah 9 • Pindaan para 7.3.2 (b): pengguna perlu menukarkan kata laluan setiap enam (6) bulan. • Pindaan para 7.3.3 (a) ID dan capaian logikal hanya boleh diberi selepas borang permohonan diisi dengan lengkap oleh pengguna, disokong atau disahkan oleh Pengurus pemohon. • Pindaan para 7.3.4 (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*). • Pindaan para 7.3.5 (a) Semua log atau *audit trail* hendaklah diaktifkan untuk merakamkan kegunaan ID dan hak capaian. Log tersebut perlu disemak oleh Pentadbir Aplikasi/ Sistem/ Aset ICT dari masa ke semasa untuk memastikan kegunaan sistem dengan betul dan teratur dan tidak ada unsur mencurigakan.
		Seksyen 8.Pembangunan dan Penyelenggaraan Aplikasi	• Perubahan Tajuk 8.3.2

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			• Penambahan Para 8.3.4 Perancangan dan Penerimaan Sistem
		Seksyen 9. Pengurusan Insiden	• Pindaan para 9.1 : Tujuan dan Skop Polisi 'Pengurusan Insiden' bertujuan untuk memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT. • Pindaan para 9.2 : Penyataan Polisi Insiden Keselamatan ICT hendaklah dilapor dan diselesaikan melalui Pentadbir Sistem ICT secara terkawal dan tepat. Insiden yang dilapor hendaklah dipantau dan dilapor kepada CIO dan ICTSO Jabatan/ Agensi secara berkala. • Tambahan penerangan di para 9.3 a. Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. b. Sembilan (9) jenis insiden yang dikenalpasti mengikut Surat Pekeliling Am Bilangan 4/2006 adalah seperti berikut : i. Pelanggaran Dasar (Violation of Policy) - Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT.

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			ii. Penghalangan Penyampaian Perkhidmatan (Denial of Service) - Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk denial of service (DoS), distributed denial of service (DDoS) dan sabotage. iii. Pencerobohan (Intrusion) - Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan manamana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (system tampering), pindaan data (modification of data) dan pindaan kepada konfigurasi sistem. iv. Pemalsuan (Forgery) - Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage) dan penipuan (hoaxes). v. Spam - Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan. vi. Malicious Code - Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya. vii. Harrassment/Threats - Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu. viii. Attempts/Hack Threats/Information Gathering - Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk spoofing, phishing, probing, war driving dan scanning. ix. Kehilangan Fizikal (Physical Loss) - Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan. • Pindaan para 9.3.1 : Mekanisma Pelaporan a. Tindakan ke atas insiden yang berlaku hendaklah dibuat

			berasaskan kepada keparahan sesuatu insiden. b. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut : i. Keutamaan 1 (Merah) – insiden keselamatan ICT yang membawa ancaman nyawa, menggugat keselamatan dan pertahanan negara, menjejas ekonomi dan imej negara, yang mungkin memerlukan Pelan Pemulihan Perkhidmatan (BCP) diaktifkan. ii. Keutamaan 2 (Kuning) – insiden keselamatan ICT selainnya seperti pencerobohan laman web, gangguan sistem dan pencerobohan aset ICT. c. Semua pemilik aset atau Pentadbir Aplikasi/ Sistem/ Aset ICT hendaklah melaporkan insiden keselamatan ICT yang berlaku kepada Pasukan CERT Negeri Melaka di *cert@melaka.gov.my*. Pengendalian insiden keselamatan ICT hendaklah merujuk kepada SOP yang berkuatkuasa di Agensi/ Jabatan masing-masing. d. Sekiranya Jabatan/ Agensi tiada SOP untuk dirujuk Jabatan/ Agensi boleh menggunakan Borang D untuk merekod insiden yang berlaku dan Borang E untuk pemantauan penyelesaian laporan insiden. Rajah 10 adalah untuk proses menyelesaikan insiden yang merujuk kepada penggunaan Borang D, manakala

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			Rajah 12 adalah Proses Semakan Laporan Insiden. • Para 9.3.2 dipadam
		Borang	Pindaan Tajuk : Borang Akuan Pematuhan Dasar Keselamatan ICT Pindaan Borang C: Borang Permohonan/ Perubahan Sistem/ Operasi ICT
9	21 Feb 2022	VI. Penilaian Risiko Keselamatan ICT	Pindaan Para 1
		VIII.Kategori Sistem Dan Aplikasi Di Kerajaan Negeri Melaka	Pindaan Jadual 1: Sistem atau Aplikasi Penting dan Kritikal - Kategori 1
		Seksyen 5. Kawalan Fizikal dan Persekitaran	Pindaan Para 5.3.1 f(ii), f (vii), f(viii) dan (g) Pindaan Para 5.3.2 (b) Pindaan Para 5.3.3 (a) dan (b)
		Seksyen 6.Pengurusan Operasi dan Rangkaian	Pindaan 6.2: Para 4 Pindaan 6.3.1.4 a (i) dan a (iii) Para 6.3.1.4 (c) dipadam Pindaan Para 6.3.1.4 (d) Pindaan Para 6.3.3 (a) Pindaan Para 6.3.7 (h) Pindaan Para 6.3.8 (c) Pindaan Para 6.3.9 (a),(b),c,dan (d) Pindaan Para 6.3.10 a(i) a(ii), c(i) Pindaan Para 6.3.11 (a), (b) Pindaan Para 6.3.12 (a),(b) dan (c) Pindaan Para 6.3.13 a (iv)
		Seksyen 7. Kawalan Capaian Logikal	Penambahan para 7.3.2 (f) dan 7.3.2 (g)

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		Seksyen 9. Pengurusan Insiden	Pindaan Para 9.3 (a) Pindaan Para 9.3.1(c) dan 9.3.1 (e)
		Seksyen 10. Pengurusan Kesinambungan Perkhidmatan	Para 10.3.2 (b) dipadam Pindaan para 10.3.3 (d)
		Borang	Pindaan Borang C: Borang Permohonan/ Perubahan Sistem/ Operasi ICT Pindaan BORANG D: Laporan Insiden/ Masalah
10.	11 Ogos 2023	VII.Dokumen Rujukan	Pindaan Para (b), Para (g), para (l)
		VIII. Kategori Sistem Dan Aplikasi Di Kerajaan Negeri Melaka	Pindaan Jadual 1: • Pindaan Para 11 • Penambahan Para 13
		XI.Penerangan Terminologi Fungsi	Pindaan Jadual 2: Terminologi Fungsi/ Peranan dan Bidang Tugas di Para (1)
		Seksyen 1. Polisi Keselamatan Maklumat	Pindaan Para 1.2
		Seksyen 2. Pengurusan Keselamatan Maklumat	Pindaan di Para 2.4 (c) Pindaan di Para 2.5 (7) Pindaan di Para 2.7
		Seksyen 3. Pengurusan Aset Berkaitan Maklumat	Pindaan di Para 3.4 (c)
		Seksyen 4. Keselamatan Sumber Manusia	Pindaan di Para 4.3.3 (c) Pindaan di Para 4.33 (f) Para 4.3.3 (d) dan (e) dipadam Pindaan Para 4.3.6 (c)
		Seksyen 5. Kawalan Fizikal dan Persekitaran	Pindaan di Para 5.3.1 (b)
		Seksyen 6. Pengurusan Operasi dan Rangkaian	Pindaan Para 6.3.1.1(b) Pindaan Para 6.3.1.2 (a), (b) dan (c)

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
			Para 6.3.1.3 dipadam Pindaan Para 6.3.3 (b) Pindaan Para 6.3.3 (c) Para 6.3.4(c) dan (d) dipadam Pindaan Para 6.3.5 (a) , 6.3.5a (i) Pindaan Para 6.3.5 (d) Para 6.3.6 (d) dipadam Pindaan Para 6.3.7 (f) dan (j) Para 6.3.8 (b) dipadam Pindaan Para 6.3.9 (a), (b),(c), (d) dan (e) Pindaan Para 6.3.12 (b) Para 6.3.12 (c), (d) dan (e) dipadam
		Seksyen 7. Kawalan Capaian Logikal	Para 7.3.2 c (iv) dipadam Pindaan Para 7.3.2 (e) dan (f)
		Seksyen 9. Pengurusan Insiden	Pindaan Para 9.1 Pindaan Para 9.2 Pindaan Para 9.3 (a) dan 9.3 (b) Pindaan Para 9.3.1 (a), (b), (c) , (d) dan (e)
11.	8 April 2024	VIII. Kategori Sistem Dan Aplikasi Di Kerajaan Negeri Melaka	Pindaan di Jadual 1:Pindaan di Para 1 dan penambahan MD2C di Para 13
		Seksyen 2. Pengurusan Keselamatan Maklumat	Pindaan Rajah 1 Pindaan di Para 2.4f(iii), 2.4(g), 2.4(h) dan 2.4 (i)
		Seksyen 3. Pengurusan Aset Berkaitan Maklumat	Pindaan di Para 3.3(f) Pindaan Rajah 3 Pindaan di Para 3.4(d)
		Seksyen 4. Keselamatan Sumber Manusia	Pindaan di Para 4.3.3(d) dan 4.3.3(e) Pindaan di Para 4.3.5(a) dan 4.3.5(c) Pindaan di Para 4.3.6(b) dan 4.3.6(c) Para 4.3.6(f) dipadam

Bil.	Tarikh	Bahagian Yang Berkenaan	Keterangan Perubahan
		Seksyen 6. Pengurusan Operasi dan Rangkaian	Pindaan di Para 6.3.1.2(b) Pindaan di Para 6.3.1.3a (i) dan 6.3.1.3f (ii) Pindaan di Para 6.3.1.4 (c) dan 6.3.1.4 e (i) Pindaan di Para 6.3.2(a) Pindaan di Para 6.3.3(c), 6.3.3(d) dan 6.3.3(g) Pindaan di Para 6.3.4a(v) Pindaan di Para 6.3.5(f) Pindaan di Para 6.3.6(c) Pindaan di Para 6.3.7(g) Pindaan di Para 6.3.12(b) Pindaan di Para 6.3.13 (b)
		Seksyen 7. Kawalan Capaian Logikal	Penambahan Para baharu di para 7.3.2(b): Pengguna tidak digalakkan untuk menggunakan kemudahan pengurus kata laluan bagi mengelakkan risiko penyalahgunaan capaian; Pindaan Para 7.3.2 (b)
		Borang G	Pindaan di Para 2

I. PENGENALAN

Dokumen Dasar Keselamatan ICT Negeri Melaka (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 semua Jabatan Kerajaan Negeri Melaka (Kerajaan Negeri). Walau bagaimanapun, jabatan/ agensi boleh menggunapakai Dasar Keselamatan ICT atau prosedur 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 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 DASAR KESELAMATAN ICT

Objektif Dasar 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 DASAR KESELAMATAN ICT NEGERI MELAKA

Dasar 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

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

V. SKOP DASAR KESELAMATAN ICT NEGERI MELAKA

Skop DKICT merangkumi pengurusan, pengendalian dan penyelenggaraan aset ICT yang terdiri daripada perkakasan, perisian, perkhidmatan, data/ maklumat dan manusia.

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

VI. PENILAIAN RISIKO KESELAMATAN ICT

Kerajaan Negeri Melaka dan jabatan/ agensi di bawah pentadbiran Kerajaan Negeri Melaka hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan yang semakin meningkat hari ini. Justeru itu, Jabatan/ agensi yang berkenaan perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

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

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

Jabatan/ agensi perlu mengenalpasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

1. Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
2. Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi ;

3. Mengelak dan/ atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
4. Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

VII. 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 (Semakan dan Pindaan 2017);
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 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam;
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) Portal Pekeliling Perbendaharaan (PPP)
m) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) ; dan
n) Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

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 • Orang Awam	Hebahan maklumat dan interaksi antara rakyat dan Kerajaan Negeri Melaka
3.	Sistem e-MMKN	Semua Jabatan	Pengurusan risalat untuk Majlis Mesyuarat Kerajaan Negeri
4.	Sistem e-Tanah	• Pentadbiran Tanah Negeri Melaka • Orang Awam	Urusan berkaitan tanah dan percukaian
5.	Sistem Perakaunan dan Kewangan Standard - iSPEKS	Semua Jabatan	Pentadbiran kewangan, akaun dan pembayaran secara elektronik
6.	Gerbang Pembayaran Bersepadu Kerajaan Negeri Melaka	• Semua jabatan/ Agensi • Orang Awam	Terimaan bayaran secara elektronik dari orang awam

Bil.	Sistem atau Aplikasi Penting dan Kritikal	Kegunaan	Proses Yang Disokong
7.	Sistem Penganugerahan Darjah Kebesaran Negeri Melaka	• Jabatan Ketua Menteri Melaka • Orang Awam	Urusan penganugerahan Darjah, Tauliah, Bintang dan Pingat Kebesaran Negeri Melaka
8.	E-mel dan Kalendar Rasmi Kerajaan Negeri Melaka	Semua Jabatan	E-mel dan kalendar
9.	Sistem e-TAPEM	• Tabung Amanah Pendidikan Negeri Melaka • Institusi Pendidikan • Pelajar	Urusan bantuan dan pinjaman pelajaran anak Negeri Melaka
10.	Perkhidmatan Web/ Application Hosting	Semua Jabatan	Menyediakan perkhidmatan *hosting* bagi web dan aplikasi Jabatan/ Agensi
11.	Islamic Education Management System (IEMS)	• Jabatan Agama Islam Melaka (JAIM) • SRA dan Tadika JAIM • Orang Awam	Pendaftaran Pelajar,pengurusan markah, disiplin, pengurusan SPBT,Modul kehadiran dan cuti guru
12.	Sistem Tender Online Melaka (STOM)	• Semua Jabatan • Orang Awam	Pembelian dokumen tender dan sebut harga secara online
13.	Melaka Digital Command Centre (MD2C)	• Pengurusan Atasan • Agensi	Pusat Pengurusan maklumat digital bersepadu

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

IX. TANGGUNGJAWAB

Semua kakitangan Kerajaan Negeri dan pembekal 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 Dasar 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 DKICT yang memungkinkan tindakan disiplin.

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	:	<ketuaict>@melaka.gov.my

<ketuaict> 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 Digital (CDO)	Ketua Pegawai Digital bertanggungjawab meneraju inisiatif pendigitalan di Jabatan melalui penggunaan data, analitis dan teknologi digital; dan Mewujudkan budaya berpacukan data yang mengamalkan pendekatan *principle-based* melalui penggunaan data dan teknologi digital.
2.	Pegawai Keselamatan ICT (atau ICTSO Jabatan)	Pegawai Keselamatan ICT Jabatan bertanggungjawab ke atas keseluruhan pematuhan DKICT Negeri Melaka. 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 DKICT.
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 DKICT.
6.	Jawatankuasa Pemandu Teknologi	Jawatankuasa ini menentukan hala tuju pelaksanaan ICT Negeri Melaka, menetapkan DKICT dan memantau

Bil.	Nama Peranan	Keterangan Bidang Tugas
	Maklumat Negeri Melaka	tahap pelaksanaan serta pematuhan DKICT 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 Pemilik Aplikasi/ Sistem dalam penyelesaian masalah atau insiden.
9.	Khidmat Bantuan Tahap 2	Bantuan daripada pihak yang membekalkan aplikasi/ sistem.
10.	Pemilik Aset	Ketua Jabatan/ Agensi yang bertanggungjawab terhadap pemilikan aset bagi pihak kerajaan.
11.	Pemilik Aplikasi/ Sistem	Pemilik Aplikasi/ Sistem adalah pembekal aplikasi/ sistem tersebut. Pemilik bertanggungjawab atas semua pembetulan fungsi dan naiktaraf aplikasi/ sistem.
12.	Pengguna Aset	Kakitangan yang bertanggungjawab terhadap keselamatan aset untuk kegunaan harian.
13.	Pemilik Data	Pegawai Jabatan/ Agensi yang berkepentingan terhadap kerahsiaan dan kesahihan data yang disimpan
14.	Pengguna-pengguna	Pegawai/ kakitangan yang menggunakan aplikasi/ sistem dan aset bagi urusan rasmi.
15.	Pengurus Aplikasi/ Sistem	Pegawai yang bertanggungjawab terhadap pembangunan, naik taraf dan pembetulan aplikasi/ sistem.

Bil.	Nama Peranan	Keterangan Bidang Tugas
16.	Pentadbir Aplikasi/ Sistem/ Aset ICT	Pentadbir Aplikasi/ Sistem/ Aset ICT bertanggungjawab: i) memastikan aplikasi/sistem berjalan dengan lancar, ii) melaksanakan konfigurasi aplikasi, iii) peruntukkan sumber CPU dan memori (*CPU and memory resources*), iv) instalasi *patches*, v) naik taraf (*upgrade*), dan vi) menjana dan mengemaskini log. vii) 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; viii) Menyiasat cubaan capaian yang gagal dan mencurigakan (*suspicious failed login attempts*) serta mengambil tindakan sewajarnya, jika perlu; ix) Melaksanakan perubahan konfigurasi pangkalan data sekiranya diminta oleh pembekal sistem; x) Menjana log akses dan perubahan data jika perlu, dan membersihkan log dari semasa ke semasa; xi) Melakukan *tuning* termasuk *reindexing* apabila diperlukan; dan xii) Memberi hak capaian pangkalan data untuk aplikasi (dan bukan kepada pengguna) dan fungsi bagi *backup* dan pemulihan (*recovery*).

Bil.	Nama Peranan	Keterangan Bidang Tugas
17.	Pentadbir Pangkalan Data	Pentadbir Pangkalan Data adalah fungsi teknikal yang bertanggungjawab i) memastikan pangkalan data berfungsi dengan baik dan dikemaskini dari semasa ke semasa, ii) melaksanakan perubahan pangkalan data mengikut keperluan, dan iii) menjana dan mengemaskini log.
18.	Pentadbir Keselamatan	Pentadbir Keselamatan bertanggungjawab memastikan tahap keselamatan terhadap aset ICT sentiasa berada dalam tahap optimum.
19.	Penyelaras Prosedur	Pegawai yang bertanggungjawab mengemaskini dan menyebarkan prosedur-prosedur berkaitan kegunaan, pengurusan dan penyelenggaraan aplikasi atau perkhidmatan sokongan.
20.	Pegawai Keselamatan Jabatan (CGSO)	Pegawai yang bertanggungjawab melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

Jadual 2: Terminologi Fungsi/ Peranan dan Bidang Tugas

XII. 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 pelaksanaannya 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 memandangkan pelbagai garis panduan umum berkaitan kegunaan e-mel, perlindungan virus dan seumpamanya telah wujud.)

4. Prosedur

Prosedur dikenali sebagai *operating procedure* atau *standard operating procedures* (SOP). 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. Dalam siri dokumen ini hanya prosedur-prosedur asas sahaja disediakan.

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 Maklumat 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/ Agensi 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.

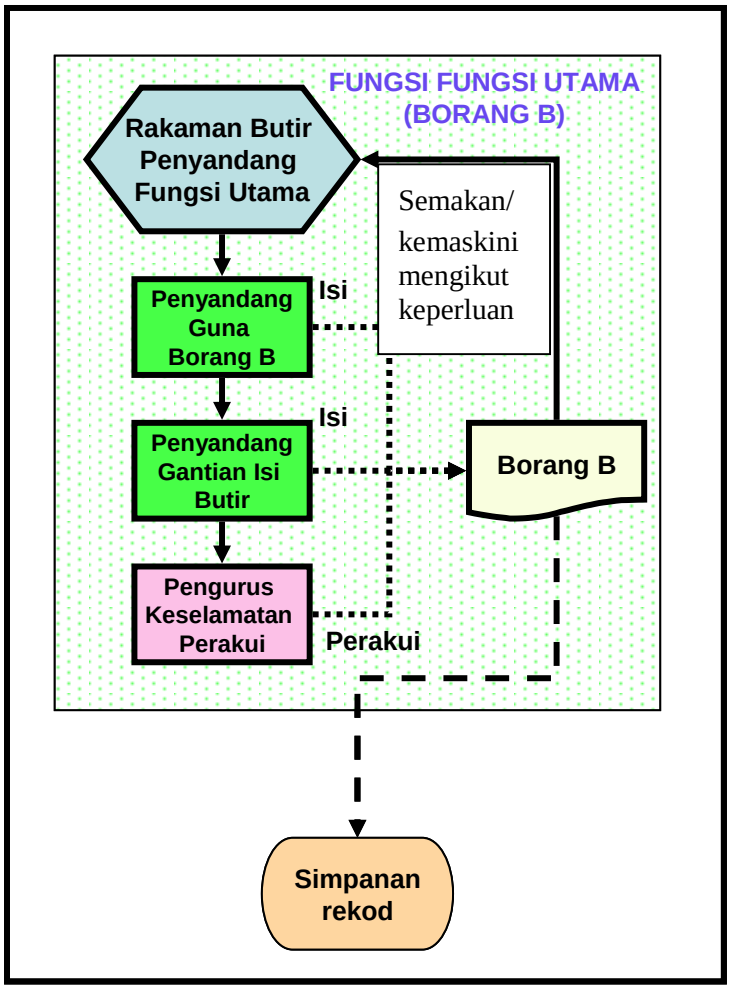
2.4. Prosedur Pengurusan Keselamatan Maklumat

a. Pegawai Keselamatan ICT Jabatan/ Agensi hendaklah mengenalpasti pegawai-pegawai yang akan memegang pelbagai fungsi seperti diterangkan di para 2.5.

b. **Untuk aplikasi dan sistem dalam Kategori 1, pengasingan tugas dan fungsi pentadbiran sistem hendaklah dikuatkuasakan.**

c. Pelaksanaan dan penguatkuasaan keselamatan ICT hendaklah dibuktikan dengan dokumen dan rekod yang berkaitan. Borang A hingga J yang dilampirkan dan diterangkan dalam LAMPIRAN 2, digunakan untuk tujuan kelulusan permohonan, pemantauan, dan juga merekod aktiviti. Borang-borang ini hendaklah dilengkapkan dan disokong dengan rekod dan laporan jejak audit yang berkaitan.

d. Setiap Jabatan dikehendaki mewujudkan piawaian tersendiri untuk Nombor Siri yang digunakan dalam tiap-tiap Borang A hingga J dan lain-lain borang khusus yang digunakan.



Rajah 1 : Proses Merekod Fungsi Utama

e. Pegawai yang menyandang atau dilantik memegang fungsi kritikal dalam pengurusan dan pentadbiran keselamatan hendaklah direkodkan dalam Borang B mengikut proses dalam Rajah 1. Perekodan juga boleh dibuat menggunakan kaedah atau format lain yang bersesuaian dengan jabatan/ agensi masing-masing.

f. Prasyarat mengisi Borang B ialah:
   i. Butiran Pegawai Utama *(Primary)* hendaklah diisi manakala butiran Pegawai Gantian *(Secondary)* digalakkan untuk diisi.
   ii. Tandatangan Pegawai perlu jelas dan terang kerana ini akan digunakan untuk perbandingan dalam borang dan dokumen yang ditandatanganinya semasa menjalankan tugas.
   iii. Apabila berlaku pertukaran, maka borang baru perlu diisi dan rekod pembatalan borang lama perlu direkodkan di sebelah bawah Borang B.
   iv. Pegawai Keselamatan ICT perlu mengesahkan penamaan dan butiran dalam Borang B.

g. Pentauliahan pegawai di para (e) hendaklah dilakukan oleh pengurusan yang lebih tinggi atau boleh juga dibuat menerusi surat lantikan daripada pengurusan atasan.

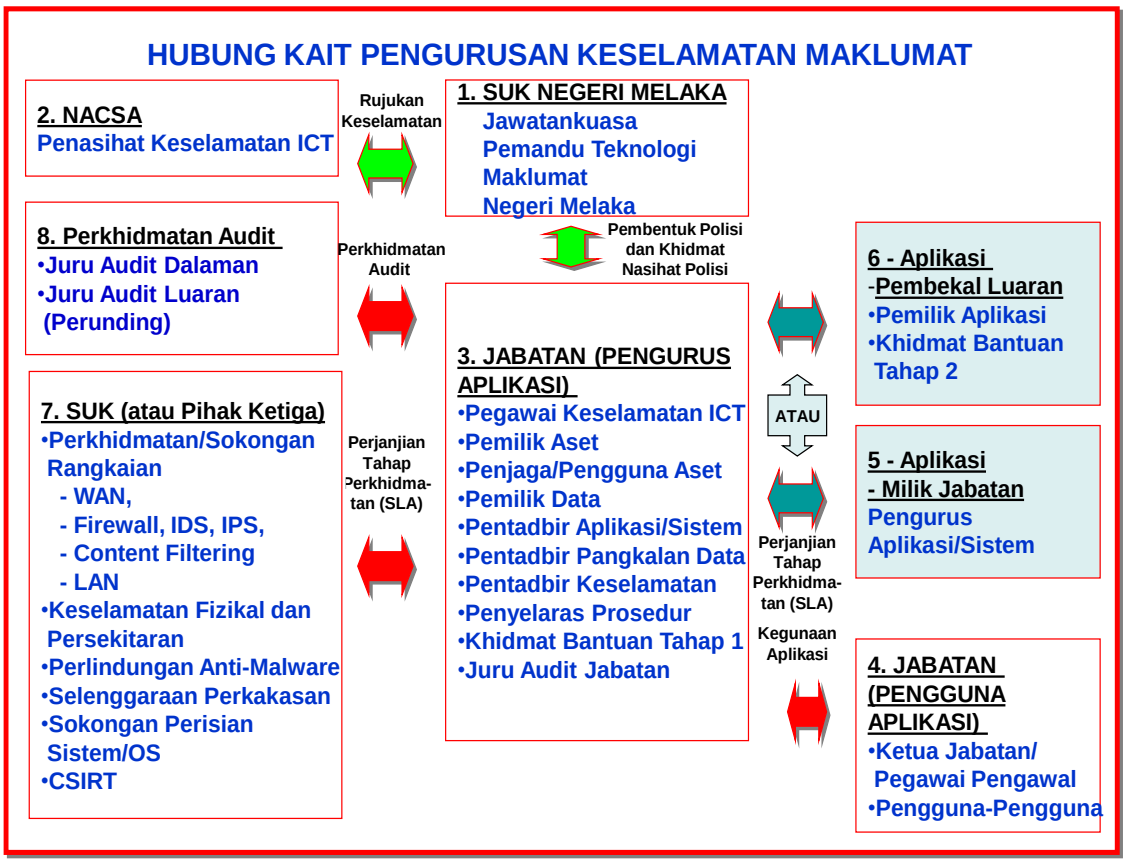
h. Tempat simpanan rekod hendaklah dikenalpasti,manakala borang dan dokumen sokongan yang telah diisi hendaklah disimpan di tempat simpanan rekod.

i. Jabatan bebas memilih tempat simpanan rekod masing-masing. Walau bagaimanapun, tempat simpanan rekod itu hendaklah direkodkan. Rekod rekod yang disimpan hendaklah:
   i. Mengikut tempoh masa yang ditetapkan bagi tujuan semakan, pemantauan atau auditan;
   ii. Dilindungi dari kecurian dan perubahan yang tidak dibenarkan; dan
   iii. Disimpan mengikut klasifikasi dokumen tersebut.

2.5. 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 2.



Rajah 2: Hubung kait Pengurusan Keselamatan Maklumat

Penerangan ringkas berkaitan Rajah 2 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 : NACSA

NACSA 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/Aset ICT, Pentadbir Pangkalan Data dan Pentadbir Keselamatan mesti diasingkan, kecuali sekiranya reka bentuk 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 berkursus. 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 aplikasi 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. \

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, pendingin hawa Pusat Data , UPS dan pelayan, bergantung kepada keperluan khusus Jabatan berkenaan.**

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

Semua perkhidmatan sokongan termasuk kegunaan WAN, *firewall*, *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.

8: Perkhidmatan Audit

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.

2.6. Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka

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

2.7. Ketua Pegawai Digital

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

a. Memastikan Pelan Strategik Pendigitalan (PSP) Jabatan/ Agensi selari dengan PSP Sektor Awam dan Pelan Strategik Jabatan/ Agensi;
b. Memantapkan struktur tadbir urus pendigitalan agensi dan menyelaras penggunaan dasar, standard dan amalan terbaik global serta menyelaras pembudayaan ICT dalam sistem penyampaian perkhidmatan jabatan.

2.8. Pegawai Keselamatan ICT

Pegawai Keselamatan ICT mesti wujud di setiap Jabatan/ Agensi. 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;

- Menimba pengalaman yang mencukupi dalam bidang keselamatan siber; dan
- Memperolehi tapisan keselamatan daripada agensi yang diberi kuasa.

Tanggungjawab ICTSO adalah seperti berikut:

a. Merancang, mengurus dan melaksanakan program keselamatan di Jabatan;
b. Memastikan Jabatan/ Agensi mematuhi Dasar Keselamatan ICT Negeri Melaka;
c. Bekerjasama dengan ICTSO Kerajaan Negeri Melaka 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.

2.9. Pegawai Keselamatan Jabatan (CGSO)

Pegawai Keselamatan Jabatan yang dilantik hendaklah terdiri daripada Timbalan Ketua Jabatan 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 dengan kerjasama Pejabat Ketua Pegawai Keselamatan Kerajaan, Jabatan Perdana Menteri bagi memastikan setiap anggota di Kementerian / 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.

2.10. 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.

2.11. Penjaga atau Pengguna Aset

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

2.12. 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.

2.13. 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.

2.14. 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.**

2.15. Pentadbir Aplikasi/ Sistem/ Aset ICT

Pentadbir Aplikasi/ Sistem/ Aset ICT hendaklah memastikan 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 instalasi *patches* dan naik taraf (*upgrade*); dan
d. Menjana dan mengemaskini log.
e. 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;
f. Menyiasat cubaan capaian yang gagal dan mencurigakan (*suspicious failed login attempts*) serta mengambil tindakan sewajarnya, jika perlu;

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

2.16. 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 mengemaskini 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*).

2.17. 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.

2.18. 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.

2.19. 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.

2.20. 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/ 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 Dasar Keselamatan ICT Negeri Melaka seperti di Lampiran 1.

2.21. 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.

2.22. 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.

2.23. 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.

2.24. Juru Audit Dalaman

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

2.25. 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 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*);
    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*).

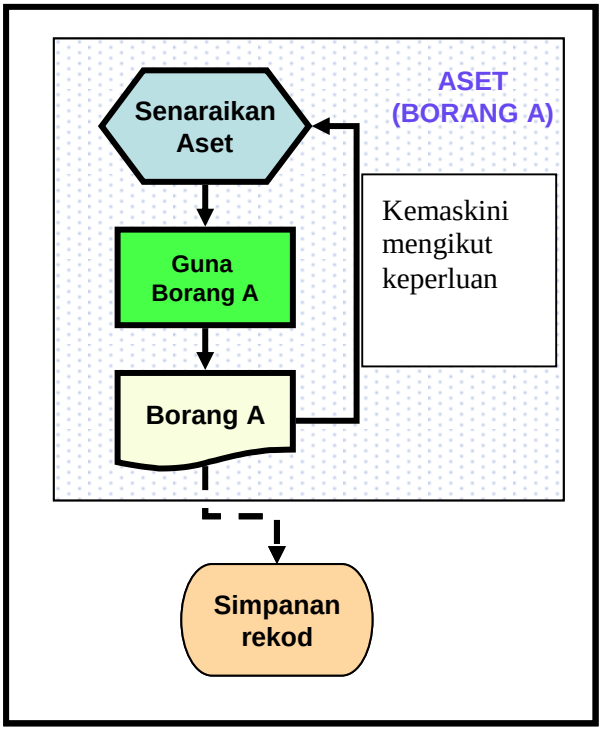
b. Aset maklumat dalam bentuk digital atau hardcopy perlu diklasifikasikan berdasarkan tahap kritikal atau kepentingan (*criticality or importance*) supaya langkah perlindungan dan pengurusan yang sewajarnya dapat diaturkan;
c. Pemilik aset maklumat bertanggungjawab mengklasifikasikan maklumat dan menyemak 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), dan *media backup* yang lain mesti dikosongkan atau dimusnahkan supaya data tidak dapat diekstrak (*extract*) oleh pihak yang tidak bertanggungjawab.

3.4. Prosedur Pengurusan Aset

a. Semua aset fizikal Jabatan yang berkaitan dengan perjalanan sistem maklumat (termasuk aset sokongan seperti pendingin hawa di Pusat Data), hendaklah direkodkan dalam borang sedia ada tetapi butiran tambahan yang perlu untuk pengurusan keselamatan ICT hendaklah direkodkan berasingan. Butiran tambahan adalah seperti berikut:
    i. Pemilik Aset (*asset owner*),
    ii. Penjaga Aset atau Pengguna Aset (*asset custodian*),
    iii. Lokasi aset,
    iv. Jangka hayat aset (sekiranya maklumat ini ada),
    v. Harga perolehan aset (sekiranya maklumat ini ada),
    vi. Hubungkait aset dengan aset lain (sekiranya maklumat hubungkait aset kurang jelas fungsinya),
    vii. Penyelenggara aset (*asset maintainer*).

b. Semua aset maklumat yang tidak direkodkan dalam borang aset Kerajaan sedia ada hendaklah direkodkan dalam Borang A dengan butir-butir berkaitan termasuk:
   i. Pemilik Aset (*asset owner*),
   ii. Penjaga Aset atau Pengguna Aset (*asset custodian*),
   iii. Klasifikasi aset (untuk aset maklumat atau data),
   iv. Lokasi aset,
   v. Jangka hayat aset (sekiranya maklumat ini ada),
   vi. Harga perolehan aset (sekiranya maklumat ini ada),
   vii. Hubungkait aset dengan aset lain (sekiranya maklumat hubungkait aset kurang jelas fungsinya),
   viii. Penyelenggara aset (*asset maintainer*).

c. Proses merekod aset menggunakan Tatacara Pengurusan Aset Kerajaan di dalam Portal Pekeliling Perbendaharaan (PPP) atau Borang A ditunjukkan dalam Rajah 3.



Rajah 3 : Proses Merekod Aset

d. Senarai aset hendaklah dikemaskini mengikut keperluan.
e. Semua kakitangan hendaklah mengendalikan aset mengikut standard yang telah ditetapkan di para 3.3.

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/ 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/ 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 Jabatan/ Agensi dan diaturkan supaya semua kakitangan diberi peluang untuk hadir sekurang-kurangnya sekali setahun.
d. Semua kakitangan hendaklah merekodkan kehadiran mereka dalam latihan.
e. Meja Khidmat Bantuan hendaklah memberi penerangan ringkas berkaitan Polisi, Standard dan Prosedur kepada pengguna..

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/ Agensi hendaklah memaklumkan kepada Pengurus/ Pemilik Aplikasi/ Sistem/ Data sekiranya terdapat kakitangan di bawah jagaannya berpindah atau bersara dan memastikan Borang J: Borang Penamatan Akaun Aplikasi Dan Pemulangan Peralatan ICT dikemukakan kepada Bahagian ICT di Jabatan/ Agensi masing-masing secara manual atau sistem yang berkaitan. Manakala Borang C digunakan bagi permohonan ID pengguna dan hak capaian untuk pegawai pengganti.
b. Bahagian ICT di Jabatan/ Agensi perlu mengambil tindakan sewajarnya dalam tempoh 14 hari dari tarikh akhir Pegawai/ Kakitangan berkhidmat.
c. Kata laluan bagi pengguna berkenaan hendaklah diubah selepas tarikh perpindahan atau persaraan kakitangan berkenaan atau ID

pengguna 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 Bahagian ICT di Jabatan/ Agensi 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 kepada Khidmat Bantuan Tahap 1 dengan menggunakan Borang D atau Sistem Aduan Kerosakan/Insiden Jabatan/Agensi masing-masing.
c. Jika laporan dibuat melalui telefon atau e-mel, maka kakitangan tersebut hendaklah menyusulinya dengan Borang D atau Sistem Aduan Kerosakan/Insiden Jabatan/Agensi masing-masing 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.

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, Pusat Data dan penjana kuasa kecemasan (*genset*);
b. Semua komputer tidak boleh ditinggalkan dalam keadaan *logged on* tanpa kehadiran pengguna; kecuali telah disetkan *auto lock* 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;
d. Semua aset yang telah disenaraikan dalam Borang A atau borang aset sedia ada kerajaan, terutamanya aset persekitaran dan keselamatan fizikal hendaklah dikenalpasti kedudukan dan kesesuaiannya untuk menyokong operasi;
e. Tempat untuk simpanan rekod-rekod pematuhan keselamatan ICT hendaklah dikenalpasti dan lokasi tersebut hendaklah dikawal;
f. 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 log 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 janakuasa tunggu sedia (*standby generator*) (jika ada) mula berfungsi atau sebelum sistem pelayan dimatikan (*shutdown*) dengan betul;
    v. Kewujudan janakuasa tunggu sedia untuk membekalkan kuasa jika perlu;
    vi. Keadaan sistem pengesan dan pencegah kebakaran yang sesuai dan berfungsi dengan baik;
    vii. Ruang khas yang selamat disediakan untuk menyimpan *media backup*; dan

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

g. Pelawat atau 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/ Agensi 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 diiring oleh kakitangan yang dibenarkan. Maklumat keluar masuk pelawat mesti direkodkan dalam buku log pelawat di tempat 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 selamat dari ancaman kebakaran atau bencana lain;
b. Pergerakan semua media storan dari suatu tempat ke tempat lain perlu direkod 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.

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 secara *public* yang disediakan di Jabatan Kerajaan Negeri Melaka adalah untuk kegunaan orang awam dan peralatan mudah alih kakitangan. Manakala penggunaan rangkaian tanpa wayar secara local atau *private* adalah tidak dibenarkan kecuali dengan kelulusan dan mesti

mematuhi syarat-syarat yang ditetapkan oleh Pegawai Keselamatan ICT Kerajaan Negeri ICTSO.

6.3. Standard dan Prosedur Pengurusan Operasi dan Rangkaian

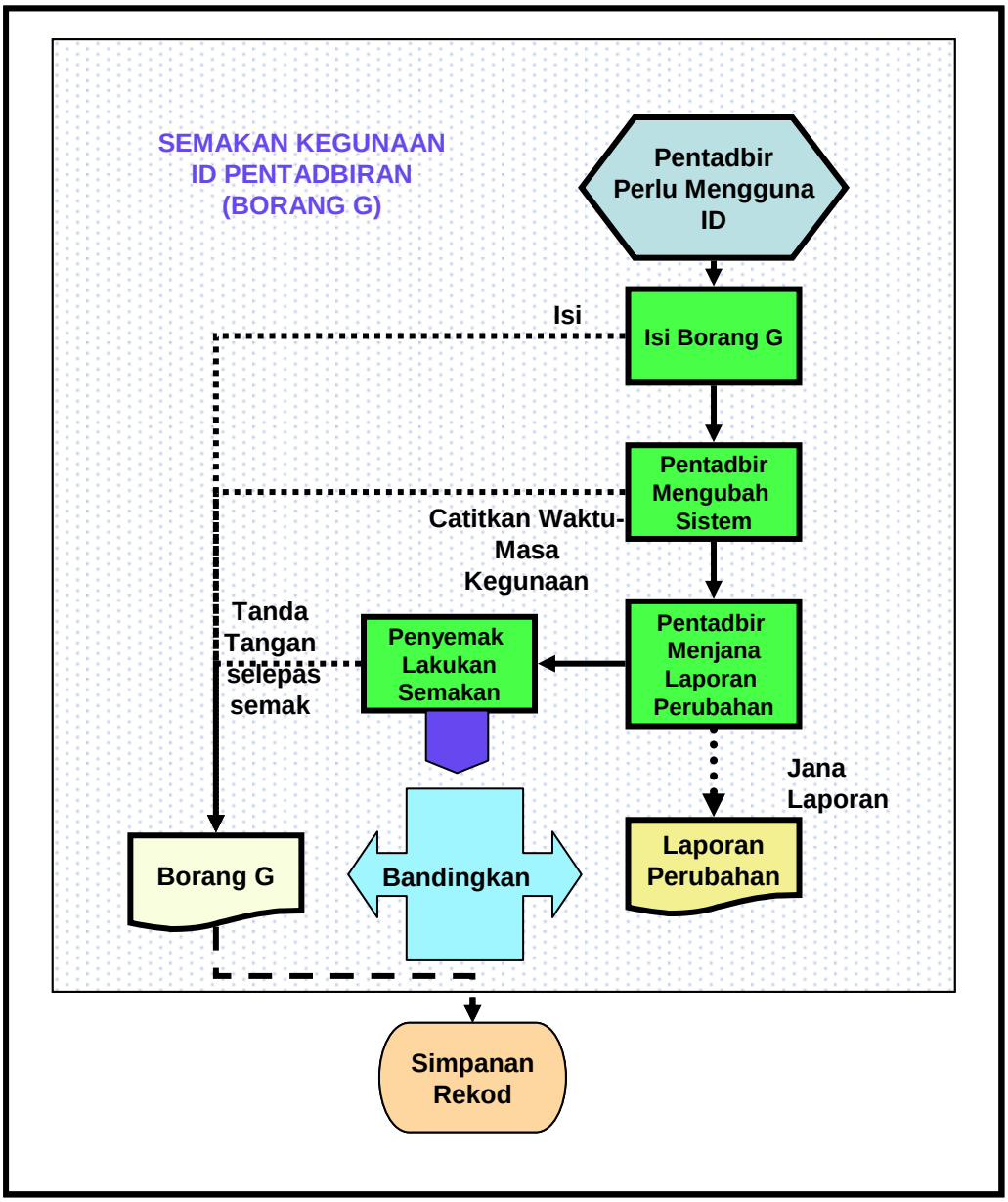
6.3.1. Pengurusan Konfigurasi

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 naik taraf; 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/ Pengurus Aset. Pemilik/ Pengurus Aset akan mempertimbangkan permohonan atau cadangan perubahan konfigurasi selepas mengambilkira:
   i. Asas keperluan perubahan;
   ii. Peruntukan sumber (*resource allocation*) ;

6.3.1.2. Pengurusan Konfigurasi Perkakasan

a. Konfigurasi perkakasan, perisian dan rangkaian hendaklah direkod untuk rujukan sekiranya berlaku insiden atau masalah;
b. Perubahan konfigurasi perkakasan tersebut perlu dilakukan dengan menggunakan ID Pentadbiran yang direkodkan, menggunakan Borang G mengikut prosedur dalam Rajah 4 atau kaedah lain yang bersesuaian; dan
c. Rekod-rekod perubahan konfigurasi hendaklah disimpan.



Rajah 4 : Proses Kegunaan ID Pentadbir

6.3.1.3. 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, Load Balancer, Antivirus, dan lain-lain;

ii. Alamat IP rangkaian untuk setiap segmen sedia ada seperti LAN, DMZ dan WAN sama ada secara DHCP atau statik;
iii. Rangkaian tanpa wayar secara *public* atau *private* dan *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 (*troubleshooting and rectification*).

c. Sebarang permohonan perubahan polisi hendaklah dimohon oleh Pentadbir Sistem sendiri kepada Penjaga Aset dengan menggunakan Borang C atau sistem;

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

e. Rekod perubahan konfigurasi hendaklah disimpan;

f. 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 direkodkan oleh pelaksana perubahan untuk disemak oleh Penjaga Aset selepas perubahan dilaksanakan.

6.3.1.4. Perubahan Konfigurasi Sementara

a. Semua permintaan perubahan konfigurasi sementara hendaklah disalurkan kepada Penjaga Aset menggunakan Borang C untuk pertimbangan dan kelulusan. Di antara 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. Perubahan sementara juga tertakluk kepada prosedur seperti Rajah 4**;**
c. Permohonan **perubahan sementara boleh dibuat atas keperluan** penyelesaian insiden atau masalah yang dilaporkan melalui Sistem Aduan Kerosakan/Insiden Jabatan/ Agensi atau Borang D;
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 direkodkan oleh pelaksana perubahan 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.

6.3.1.5. 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. Perubahan kecemasan tertakluk kepada prosedur seperti dalam Rajah 4, yang membenarkan Borang G digunakan selepas masalah diselesaikan;
c. Permohonan perubahan kecemasan juga boleh dilakukan atas keperluan penyelesaian insiden atau masalah yang dilaporkan melalui Borang D;
d. 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;
e. **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;**
f. **Untuk aplikasi atau sistem dalam Kategori 1, semua perubahan konfigurasi hendaklah direkodkan selepas pelaksanaan (*retrospectively*) dan semua jejak audit perlu disimpan untuk semakan; Jejak Audit ini hendaklah dilampirkan kepada Borang G. dan**
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

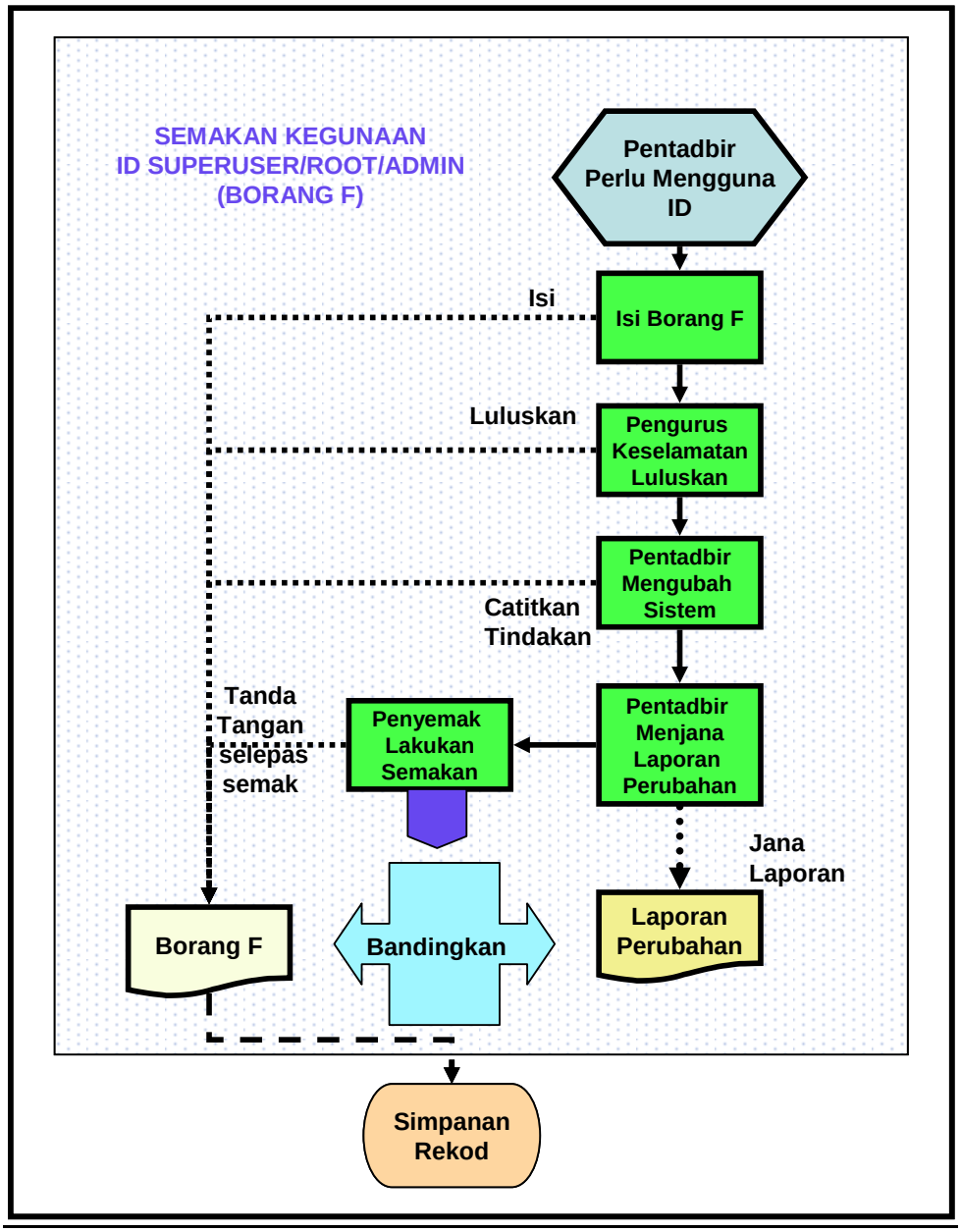
a. **Pengasingan kerja mesti dilaksanakan untuk aplikasi atau sistem dalam Kategori 1. Untuk lain-lain aplikasi atau sistem yang bukan dalam Kategori 1**, sekiranya pengasingan kerja tidak dapat dilaksanakan atas sebab-sebab tertentu, maka ID pengguna yang berasingan perlu diwujudkan dan digunakan untuk 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 dan peralatan keselamatan rangkaian. 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. ID tersebut digunakan untuk tujuan yang telah ditetapkan seperti melakukan *backup*, mengaktifkan

perkhidmatan (*services*) yang diperlukan, mengubah konfigurasi dan memantau kegunaan sistem;

c. Kegunaan ID hak capaian tinggi hendaklah direkodkan untuk semakan dari masa ke semasa melalui Borang F atau senarai yang disahkan oleh ICTSO dan disimpan di dalam almari berkunci.
d. ID khusus dan terhad hendaklah digunakan untuk penggunaan harian, manakala ID yang tinggi hak capaiannya tidak digunakan untuk tugas pemantauan dan penyelenggaraan..
e. Sekiranya ID yang tinggi hak capaiannya perlu digunakan, maka pastikan bahawa semua permohonan dan gerak langkah penggunaan dipantau menerusi proses dalam Rajah 5.



Rajah 5 : Proses Kegunaan ID Superuser/Root/Admin

f. 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/ Agensi.

g. Semua kegunaan ID yang tinggi hak capaiannya hendaklah direkodkan untuk semakan dari semasa ke semasa dan disimpan.

6.3.4. Prosedur Operasi (Operating Procedures) dan Dokumentasi

a. Semua prosedur penting berkaitan pengendalian aplikasi dan sistem hendaklah didokumen dan dikemas kini dari semasa 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. Penyelenggaraan 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. Penyelenggaraan Aplikasi atau Sistem

a. Pastikan Pengurus 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. Log transaksi dan lain-lain fail yang perlu dikemaskini dari semasa ke semasa;

ii. Penyusunan dan pengindeksan semula pangkalan data (bergantung kepada jenis teknologi pangkalan data yang digunakan dan reka bentuk 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.

e. Sekiranya jadual penyelenggaraan perlu ditangguhkan, maka aktiviti tersebut hendaklah dilakukan secepat mungkin selepas penangguhan;

f. Perkakasan yang diganti atau dibaiki hendaklah direkodkan 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 direkod jika pembekal pekhidmatan luar dipanggil untuk menyelesaikan gangguan;dan
d. 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 apabila:
    i. Aplikasi atau sistem berubah atau naik taraf; dan
    ii. Pangkalan data atau fail berubah.

f. Menyediakan jadual *backup* yang bersesuaian dengan kegunaan aplikasi;
g. Kekerapan aktiviti *backup* bergantung kepada pentingnya aplikasi atau sistem. **Untuk Kategori 1, *backup* penuh data (*full data backup*) perlu dilakukan sebulan sekali manakala *backup* data tambahan atau perubahan (*incremental or differential backup*) perlu dilakukan setiap hari.**
h. Pastikan bahawa fail penting tidak disimpan dalam komputer peribadi atau *notebook*. Ruang bagi pengguna hendaklah disediakan dalam pelayan supaya *backup* berjadual boleh dilakukan; dan
i. Pengguna hendaklah melakukan *backup* sendiri bagi fail-fail penting dan menyimpannya ditempat yang selamat.
j. Bekas media *backup*, lokasi dan infrastruktur yang menempatkan bekas media *backup* hendaklah disahkan oleh CGSO dan sebarang perubahan hendaklah mendapat pengesahan semula daripada CGSO.

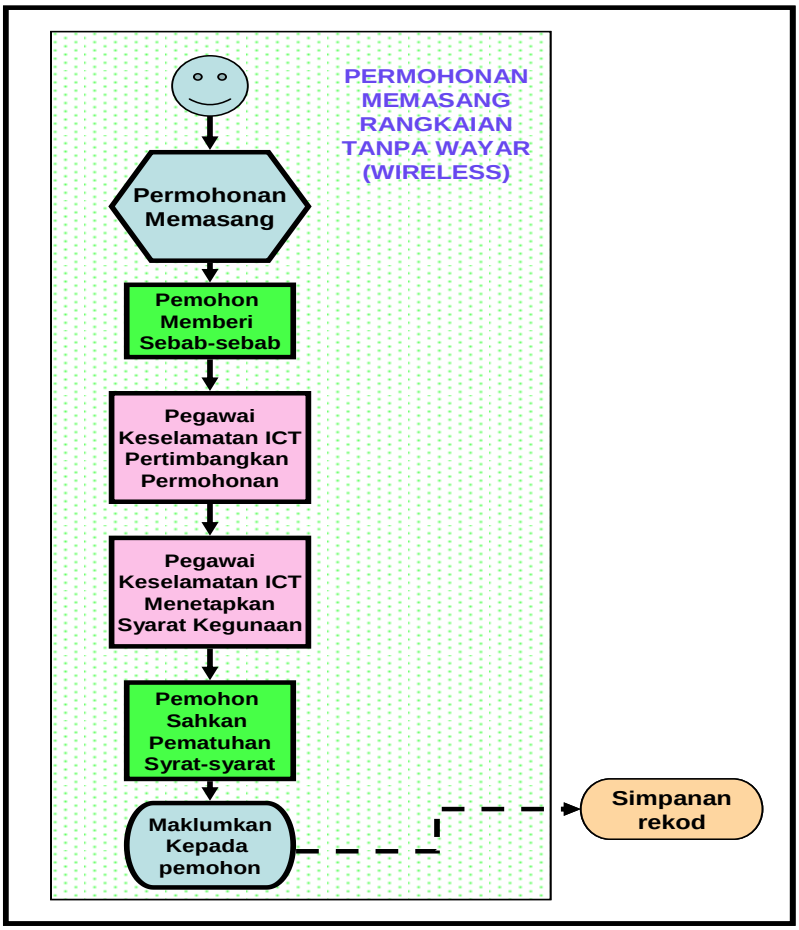
6.3.8. Komputer Kerajaan Negeri

a. 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.
b. Pengguna tidak dibenarkan mengubah pemasangan komputer atau menyambung komputer ke rangkaian lain seperti *broadband* atau *hotspot* tanpa kebenaran pihak ICT Jabatan/ Agensi.
c. Pengguna dikehendaki bekerjasama membuat ujian atau mengubah sementara sambungan ke rangkaian atas arahan

kakitangan penyelenggaraan BTMK atau ICT Jabatan/ Agensi semasa penyiasatan penyelesaian masalah secara jarak jauh (*remote*).

6.3.9. Rangkaian Tanpa Wayar

a. Rangkaian tanpa wayar yang disediakan di Jabatan/ Agensi dan tempat tumpuan awam di Negeri Melaka adalah untuk kegunaan awam.
b. Pengguna hendaklah memahami risiko dan keupayaan peralatan/ peranti mereka untuk mengakses rangkaian tanpa wayar tersebut.
c. Jabatan/ Agensi yang ingin memasang rangkaian tanpa wayar dengan menggunapakai infrastruktur rangkaian sedia ada yang disediakan oleh JKMM, hendaklah memohon kelulusan dari Pegawai Keselamatan ICT Kerajaan Negeri, melalui Ketua Jabatan/ Agensi/ Pegawai Pengawal, dengan bersurat atau e-mel dengan menyatakan justifikasi keperluan.
d. Pegawai Keselamatan ICT hendaklah bersetuju dengan permohonan keperluan, tujuan penggunaan, lokasi perkakasan, penyelenggaraan, konfigurasi IP dan cara penggunaan yang dicadangkan oleh pemohon dan menggariskan syarat-syarat yang perlu dipatuhi.
e. Pemohon hendaklah bersetuju dengan 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.
g. Aliran proses permohonan ditunjukkan dalam Rajah 6.



Rajah 6 : Proses Permohonan Rangkaian Tanpa Wayar

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 dan *Random Access Memory* (RAM); dan

   ii. Memastikan kapasiti storan mencukupi melalui penggunaan sistem pemantauan perkakasan atau hasil penyelenggaraan berkala peralatan di Jabatan/ Agensi.

b. Bahagian ICT Jabatan/ Agensi 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 Jabatan/ Agensi.

c. Di antara perkakasan yang perlu dipantau adalah seperti berikut:
   i) *CPU, RAM*:
      - 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 Antivirus

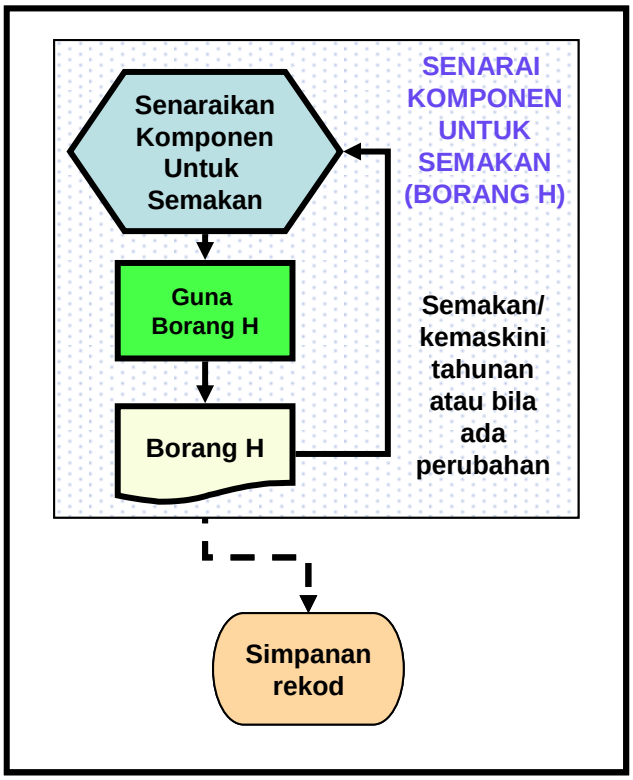
a. Bahagian ICT Jabatan/ Agensi hendaklah menetapkan perisian *antivirus* di komputer dan komputer riba milik Kerajaan Negeri atau Jabatan/ Agensi.
b. Konfigurasi pengemaskinian perisian *antivirus* hendaklah ditetapkan secara automatik atau berkala mengikut kesesuaian infrastruktur rangkaian Jabatan/ Agensi.

6.3.12. Simpanan Rekod dan Pengurusan Kualiti

a. Semua rekod penting berkaitan konfigurasi asal dan perubahan- perubahan yang dilakukan kepada aplikasi atau sistem hendaklah disimpan; dan
b. **Untuk aplikasi dan sistem dalam Kategori 1, semakan dilakukan** mengikut keperluan untuk membandingkan konfigurasi sedia ada dengan catatan rekod perubahan.

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. Penggunaan kapasiti rangkaian.
b. Senarai aktiviti, komponen atau perkara yang dianggap perlu dipantau hendaklah direkodkankan dalam Borang H/dokumen yang bersesuaian. Proses tersebut seperti Rajah 7.
c. Senarai tersebut hendaklah diluluskan oleh Pegawai Keselamatan ICT.
d. Proses semakan komponen-komponen senarai tersebut boleh dilakukan menggunakan Borang I mengikut proses seperti Rajah 8.

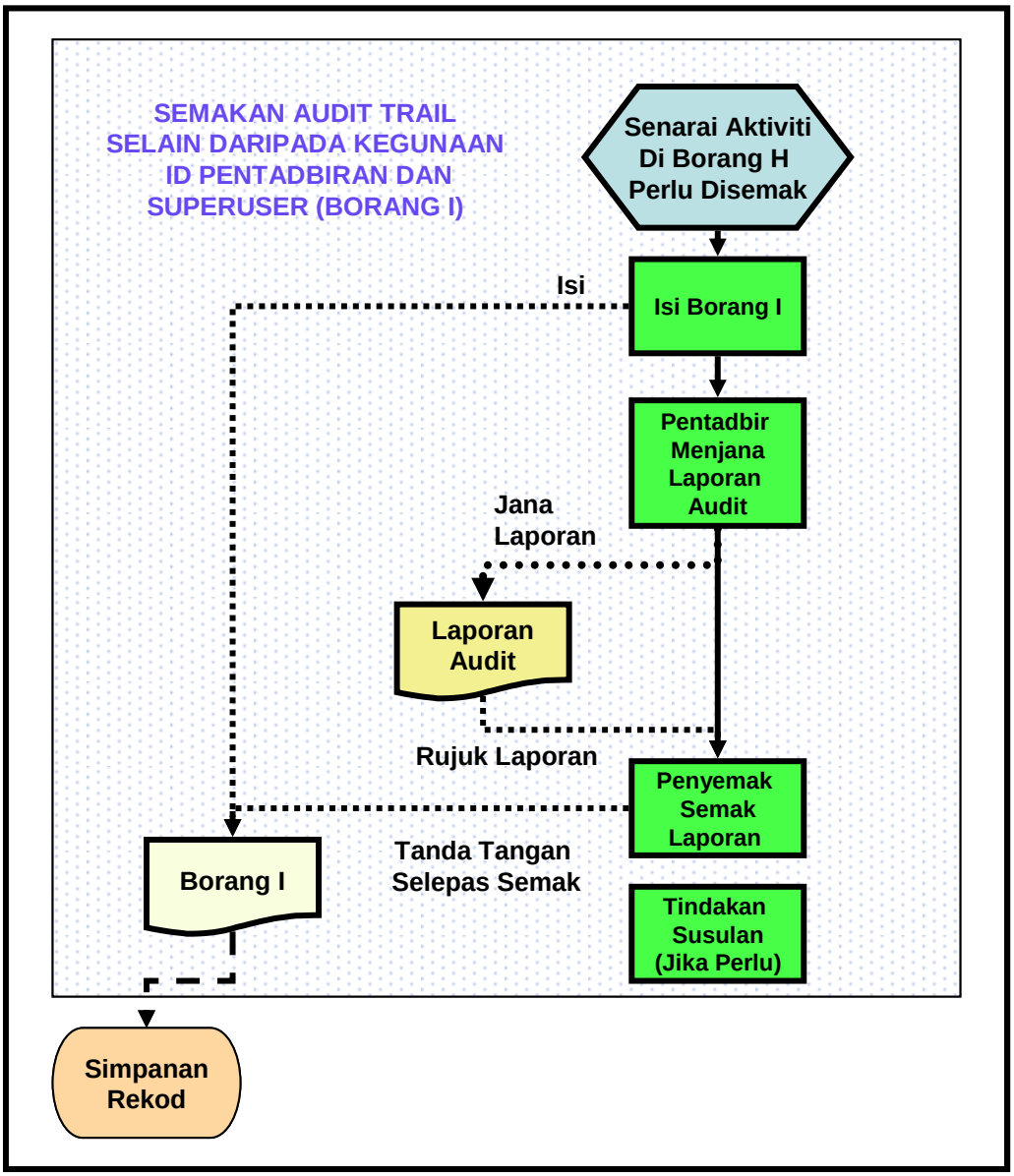


Rajah 7 : Proses Merekod Senarai Komponen Untuk Semakan

e. Borang I adalah borang umum untuk semua jenis semakan laporan dan bergantung kepada aktiviti atau komponen yang disemak.

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



Rajah 8 : Proses Semakan Komponen

6.3.15. Perkhidmatan Dalam Talian

Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

6.3.15.1 Perkhidmatan Dalam Talian

Menggalakkan pertumbuhan perkhidmatan dalam talian sebagai menyokong hasrat kerajaan mempelbagaikan saluran sistem penyampaian perkhidmatan awam

melalui aplikasi e-Kerajaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Pengenalan pengguna kepada orang awam digunakan untuk aplikasi e-Kerajaan dalam penyampaian perkhidmatan awam;

b. Maklumat yang disimpan di dalam perkhidmatan dalam talian perlu dilindungi daripada aktiviti penipuan, pendedahan dan pengubahsuaianyang tidak dibenarkan;

c. Maklumat transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi dan duplikasi; dan

d. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

6.3.15.2 Maklumat Umum

Maklumat umum merupakan hebahan maklumat yang boleh dicapai oleh orang awam melalui perkhidmatan elektronik.

a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;

b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan

c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.

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

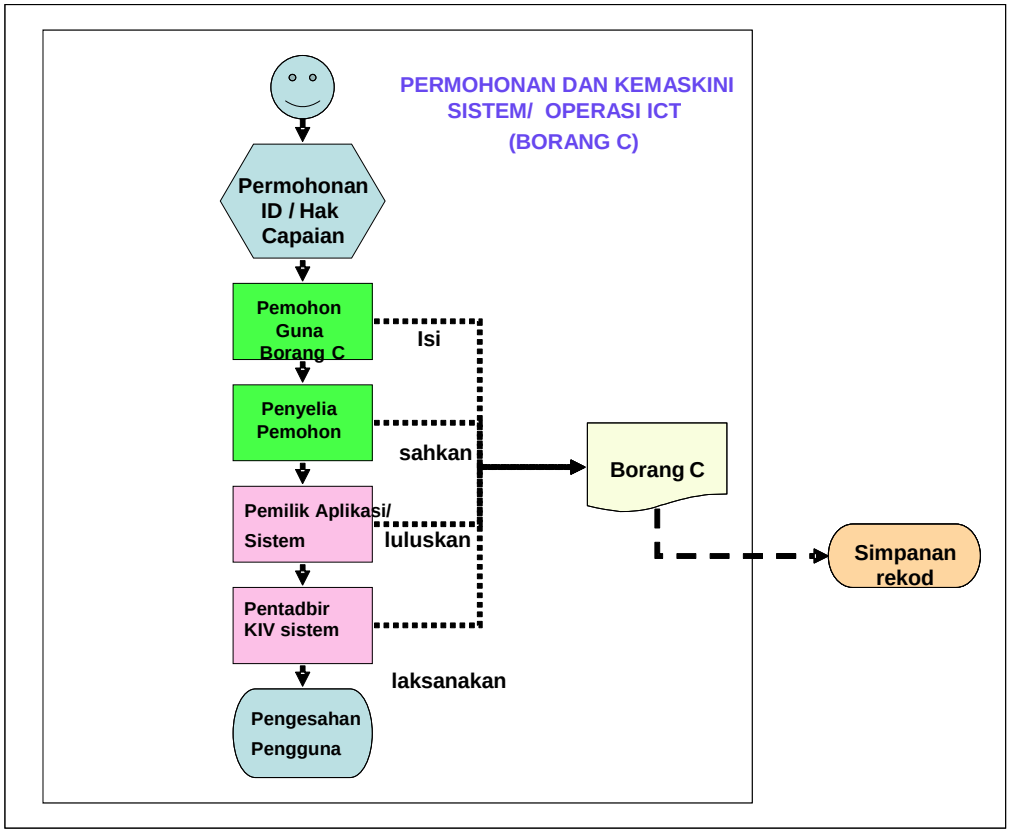
7.3.1. Kawalan Capaian Logikal Secara Umum

a. Semua sistem atau aplikasi perlu mempunyai garis panduan capaian logikal yang memaparkan keperluan atau kategori pengguna dan hak capaian yang berpatutan. Hak capaian pada umumnya diberikan atas dasar keperluan;
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 Borang C mengikut proses dalam Rajah 9 kecuali kemudahan permohonan ID yang disediakan secara *online*.



Rajah 9 : Proses Permohonan ID/ Hak Capaian dan Perubahan Aplikasi/ Sistem

7.3.2. Perlindungan Kata Laluan

a. Kata laluan mesti sekurang kurangnya mengandungi kombinasi dua belas (12) abjad dan nombor (*alphanumeric characters*);
b. Pengguna tidak digalakkan untuk menggunakan kemudahan pengurus kata laluan bagi mengelakkan risiko penyalahgunaan capaian;
c. Pengguna digalakkan menukarkan kata laluan setiap enam (6) bulan;
d. 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; dan
    iii. Apabila ID disyaki telah dicerobohi.
e. **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.
f. Sistem hendaklah berkeupayaan untuk mengawal dan memantau panjangnya kata laluan dan kekerapan kata laluan perlu ditukar.
g. Senarai kata laluan root bagi server dan appliance serta kata laluan Administrator Komputer akan diberikan kepada ICTSO serta disahkan dan disimpan di dalam kabinet berkunci setiap 6 bulan sekali.
h. ICTSO perlu mengesahkan penerimaan senarai kata laluan tersebut menggunakan buku log simpanan kata laluan.

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.

b. Pengguna-pengguna mesti memaklumkan kepada Pentadbir Aplikasi/ Sistem/ Aset ICT 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 Aplikasi/ Sistem/ Aset ICT 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.** Proses yang boleh diikuti adalah seperti dalam Rajah 8.

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*).

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 Aplikasi/ Sistem/ Aset ICT dari masa ke semasa untuk memastikan kegunaan sistem dengan betul dan teratur dan tidak ada unsur mencurigakan. 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 Aplikasi/ Sistem/ Aset ICT dari semasa ke semasa mengikut proses dalam Rajah 9 : Proses Permohonan ID/ Hak Capaian, Rajah 4 : Proses Kegunaan ID Superuser/Root/Admin dan Rajah 6 : Proses Merekod Senarai Komponen Untuk Semakan; dan

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

7.3.6. Kriptografi

a. Kriptografi merupakan alat yang penting dan asas untuk menguruskan keselamatan ICT. Objektif utama keselamatan maklumat yang dipenuhi oleh alat kriptografi asas adalah:
   i. Kerahsiaan melalui penyulitan
   ii. Integriti data melalui fungsi hash, Kod Pengesahan Mesej (MAC) atau tandatangan digital
   iii. Jaminan pengesahan sumber data melalui MAC dan tandatangan digital
   iv. Tanpa-sangkalan melalui tandatangan digital.
   v. Jaminan pengesahan entiti melalui protokol kriptografi.
b. Protokol kriptografi merupakan proses langkah demi langkah antara dua atau lebih entiti untuk mencapai matlamat keselamatan. Alat kriptografi asas digunakan dalam protokol kriptografi.
c. Pengurusan kunci kriptografi hendaklah berdasarkan penilaian risiko.
d. Algoritma kriptografi yang digunakan untuk melindungi maklumat dalam pelbagai peringkat saluran pemprosesan hendaklah mematuhi peraturan semasa yang berkuat kuasa.
e. Penggunaan Produk Kriptografi Terpercaya adalah mandatori bagi pengendalian Maklumat Rahsia Rasmi.
f. Untuk mengendalikan Maklumat Rasmi, penggunaan Produk Kriptografi Terpercaya adalah digalakkan. Produk kriptografi lain yang digunapakai oleh pihak industri juga boleh digunakan untuk mengendalikan Maklumat Rasmi.
g. Pentadbir Keselamatan perlu memastikan penggunaan kriptografi ke atas semua maklumat sensitif atau maklumat rahsia rasmi di jabatan. Contoh :
   i. Katalaluan
   ii. Transport Layer Seurity (TLS)

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 kitar hayat pembangunan dan penyelenggaraan aplikasi. Manakala tujuan prosedur adalah untuk memastikan bahawa pembangunan dan penyelenggaraan aplikasi dijalankan dengan bersistematik untuk menjamin keselamatan aplikasi.

8.2. Pernyataan Polisi

Aplikasi yang dibangunkan dan dibekalkan hendaklah sentiasa mengikut proses pembangunan standard yang mesti diurus dan disokong dengan kawalan perubahan dan pengurusan konfigurasi yang sesuai.

Kawalan yang sesuai hendaklah dibangunkan 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. Reka bentuk: 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 Aplikasi

a. Aplikasi hendaklah dibangunkan dengan mengambil kira keperluan keselamatan semasa fasa spesifikasi dan reka bentuk. 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 memastikan bahawa langkah-langkah tersebut dilaksanakan dengan betul;
c. Reka bentuk sistem hendaklah mempunyai ciri mesra pengguna (*user friendly*) supaya sistem mudah difahami oleh setiap peringkat pengguna;
d. Ciri-ciri keselamatan sistem perlu ada dalam pembangunan sistem bagi mengawal ketepatan dan integriti data. Antaranya:
    i. Penyimpanan kata laluan 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 direka bentuk mengikut garis panduan keselamatan seperti:
    i. Dokumen ISO 27002 – Code of Practice for Information Security; dan

ii. Dokumen A Guide to Building Secure Web Applications and Web Services dari OWASP – www.Owasp.org.

f. Pihak Ketiga yang membangunkan aplikasi hendaklah mendokumenkan reka bentuk aplikasi tersebut dengan ciri-ciri keselamatan seperti berikut:
   i. Penilaian keperluan keselamatan secara umum untuk keseluruhan aplikasi dan secara khusus untuk bahagian-bahagian atau modul-modul yang terdapat dalam aplikasi;
   ii. Keperluan ciri-ciri keselamatan bagi capaian aplikasi; dan
   iii. Rujukan dan sumber dokumen (seperti ISO 27002 dan OWASP) atau maklumat yang diguna untuk mendapatkan maklumat *best practices* dan keperluan lain yang terperinci yang diwajibkan atau digalakkan.

g. Sekiranya ada ciri-ciri atau fungsi keselamatan yang tidak dilaksanakan atau berbeza dari yang dicadangkan oleh rujukan-rujukan tersebut maka pembekal sistem hendaklah mengulasnya. Penerima sistem dari Kerajaan hendaklah memahami implikasi dan mengambil tindakan sewajarnya untuk bersetuju atau menguatkuasakan keperluan keselamatan yang digariskan oleh dokumen rujukan;

h. 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;

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

j. 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*); dan

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

l. Semua spesifikasi perolehan dan kontrak komersial hendaklah mengandungi keperluan mandatori seperti yang berikut :

"Kerajaan hendaklah dibenarkan untuk melaksanakan semakan terhadap kod sumber"

Untuk penyataan di atas, kerajaan adalah merujuk kepada Jabatan atau CGSO.

m. Bagi aplikasi yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori seperti yang berikut:

"Pembekal hendaklah membenarkan Kerajaan mencapai kod sumber dan melaksanakan pengolahan risiko."

Bagi penyataan di atas, kerajaan adalah merujuk kepada CGSO.

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 menggunakan Borang C;
   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.

8.3.4. Perancangan dan Penerimaan Sistem

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

8.3.4.1 Penyampaian Perkhidmatan

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan operasi sistem ICT pada masa akan datang.

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

8.3.4.2 Penerimaan Sistem

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

Seksyen 9. Pengurusan Insiden

9.1 Tujuan dan Skop

Polisi ‘Pengurusan Insiden’ bertujuan untuk memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan siber.

9.2 Pernyataan Polisi

Insiden Keselamatan siber hendaklah dilapor dan diselesaikan melalui Pentadbir Aplikasi/ Sistem/ Aset ICT secara terkawal dan tepat. Insiden yang dilapor hendaklah dipantau dan dilapor kepada CDO dan ICTSO Jabatan/ Agensi secara berkala.

9.3 Standard dan Prosedur Pengurusan Insiden

a. Insiden keselamatan Siber adalah kejadian siber yang tidak diingini apabila berlakunya kehilangan kerahsiaan maklumat, gangguan terhadap integriti data atau sistem, atau gangguan yang menyebabkan kegagalan dalam memperoleh maklumat daripada sistem komputer dan kemungkinan berlakunya kesalahan pelanggaran peraturan keselamatan maklumat, dasar-dasar tertentu atau amalan piawai keselamatan siber

b. Enam (6) jenis insiden yang dikenalpasti mengikut Surat Pekeliling Am Bilangan 4/2022 adalah seperti berikut :

   i. Penafian Perkhidmatan (Denial of Services, DoS) atau Penafian Perkhidmatan Teragih,DDoS);
   ii. Pencerobohan (Intrusion);
   iii. Jangkitan Perisian Hasad (Malicious Software, Malware);
   iv. Pengehosan Perisian Hasad (Malware Hosting);
   v. Percubaan Pencerobohan (Intrusion Attempt); dan
   vi. Potensi Serangan (Potential Attack).

9.3.1 Mekanisme Pelaporan

a. Tindakan ke atas insiden yang berlaku hendaklah dibuat berasaskan kepada keutamaan sesuatu insiden.

b. Tahap keutamaan tindakan ke atas insiden akan ditentukan seperti berikut :

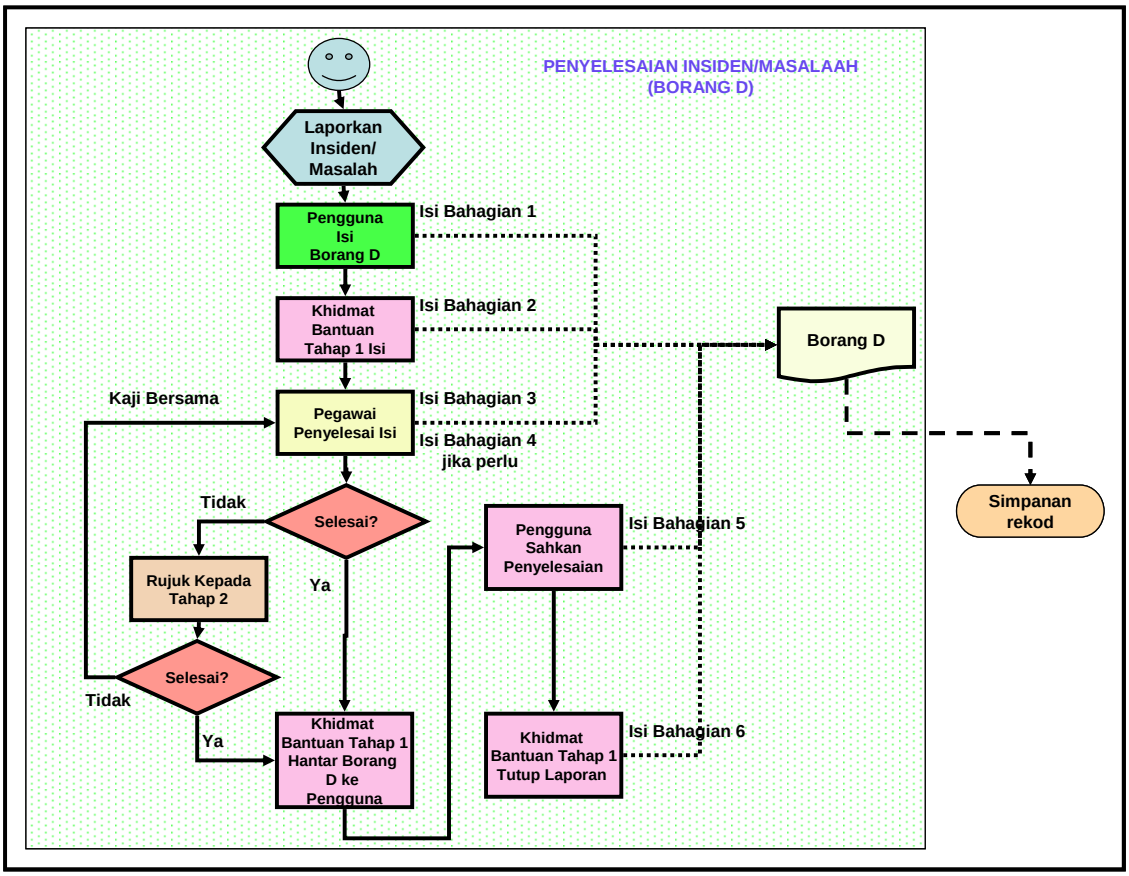
   i. Keutamaan 1– insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu; dan

   ii. Keutamaan 2 (Kuning) – insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1.

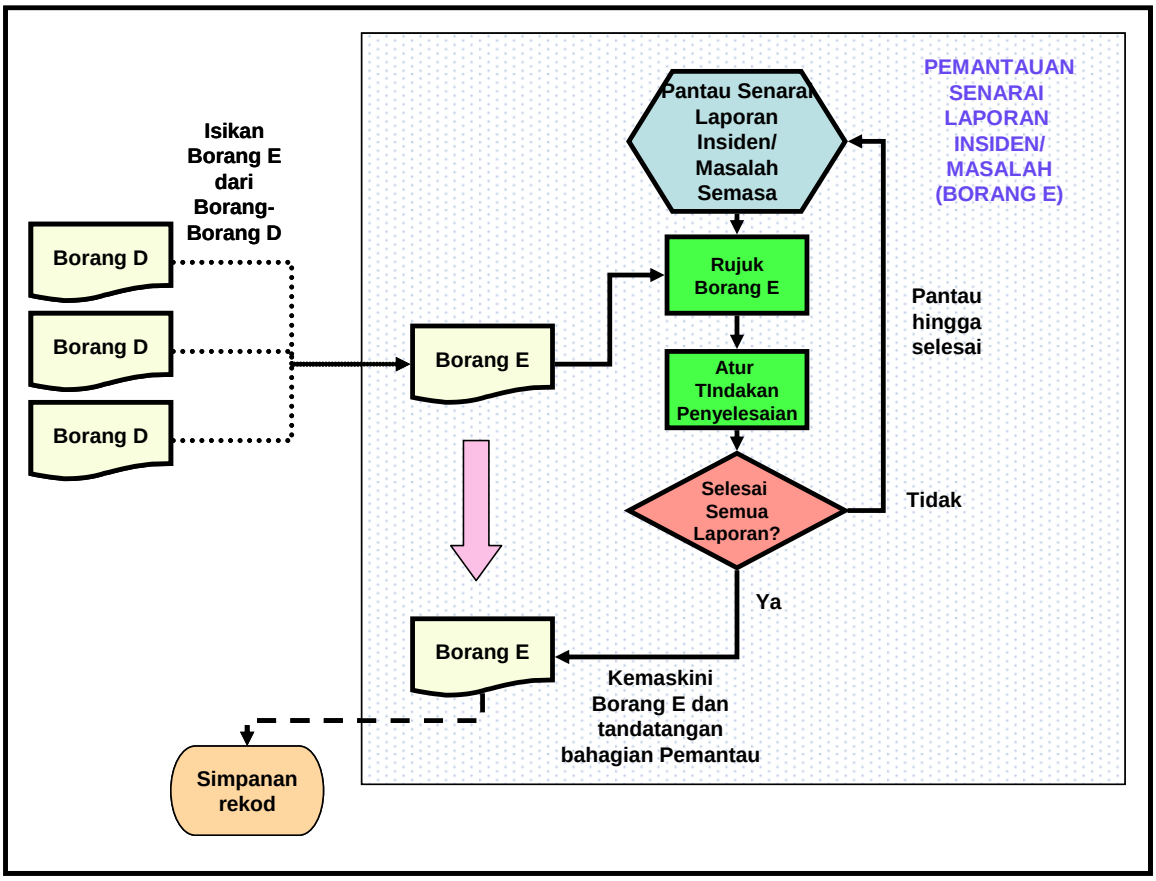
c. Semua pemilik aset atau Pentadbir Aplikasi/ Sistem/ Aset ICT Kerajaan Negeri Melaka hendaklah melaporkan insiden keselamatan siber yang berlaku ke atas Aplikasi/ Sistem/ Aset ICT dibawah kawalannya kepada Pasukan Computer Security incidence Response Team (CSIRT), ICTSO dan CDO di Jabatan/ Agensi.

d. Pengendalian dan tatacara pengurusan insiden keselamatan siber hendaklah merujuk kepada SOP yang berkuatkuasa di Agensi/ Jabatan masing-masing.

e. Sekiranya Jabatan/ Agensi tiada SOP sedia ada, Jabatan/ Agensi boleh menggunakan Borang D untuk merekod insiden yang berlaku dan Borang E untuk pemantauan penyelesaian laporan insiden. Rajah 10 dan Rajah 11 adalah untuk proses menyelesaikan insiden yang merujuk kepada penggunaan Borang D, manakala Rajah 12 adalah Proses Semakan Laporan Insiden.

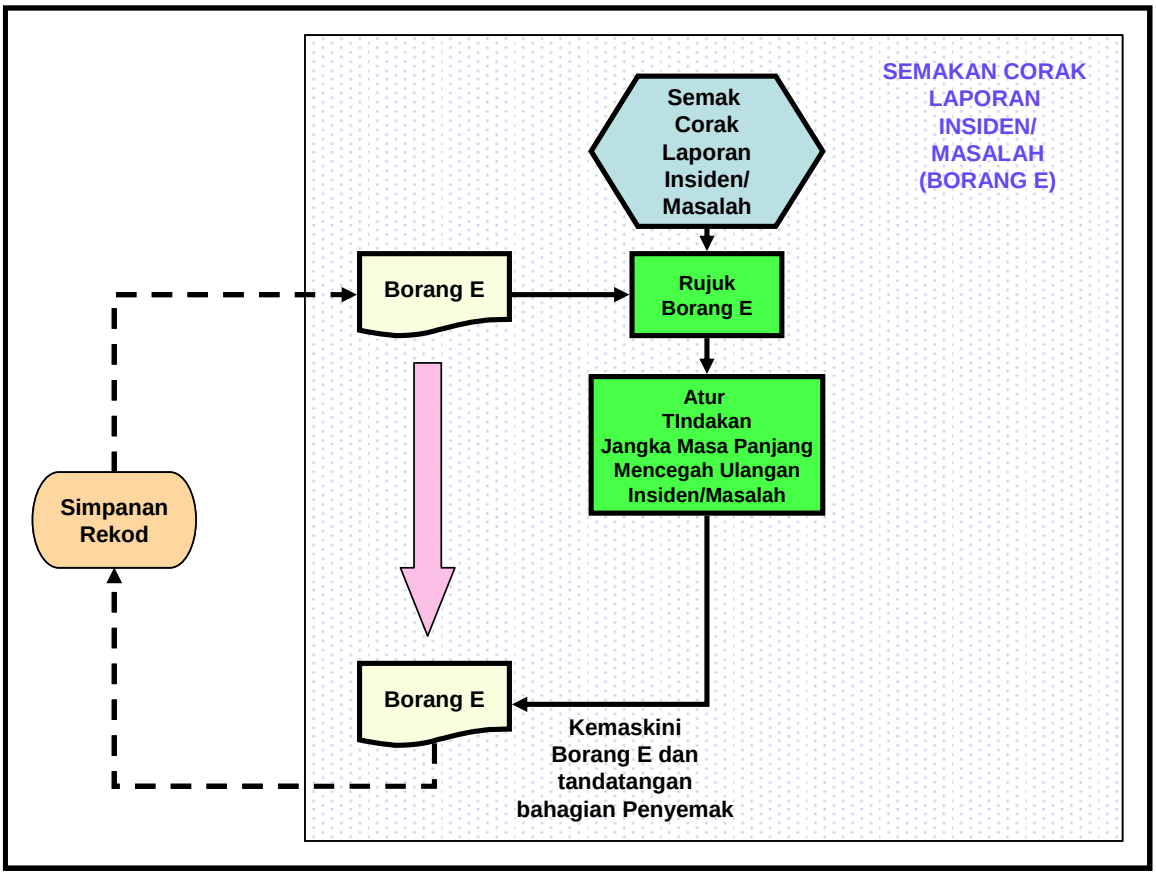


Rajah 10 : Proses Laporan Insiden dan Penyelesaian Insiden



Rajah 11 : Proses Pemantauan Penyelesaian Insiden

.



Rajah 12 : Proses Semakan Laporan Insiden

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/ Agensi 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/ 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 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 prosedur

baikpulih perkhidmatan hendaklah diperincikan apabila berlaku gangguan;

b. 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 atau simulasi hendaklah dilakukan mengikut ketetapan pengurusan.; 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/ Agensi.

11.2. Pernyataan Polisi

Reka bentuk, 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/ Agensi 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 semasa ke semasa untuk menentukan ia menepati keperluan semasa dan akan datang;
b. Semua Ketua Jabatan/ Agensi hendaklah memastikan bahawa Polisi, Standard dan Prosedur dipatuhi oleh kakitangan di jabatan/ agensi masing-masing dan merangka pelan untuk mengukur tahap pematuhan Polisi Keselamatan 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.
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/ Agensi adalah fungsi sampingan antara kakitangan terlatih dalam Jabatan/ Agensi yang mengendalikan aplikasi. Di antara fungsinya adalah:
    i. menjalankan audit pemantauan dalam Jabatan/ Agensi 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/ Agensi;

iii. tidak perlu menjalankan audit serentak untuk semua bahagian berkaitan ICT Jabatan/ Agensi, tetapi digalakkan untuk dipecahkan kepada bahagian tertentu (contoh: pengurusan rangkaian atau pengurusan semakan log sistem) untuk diaudit pada sesuatu masa; dan

iv. hendaklah dipelbagaikan untuk mengaudit bahagian-bahagian ICT yang bukan dalam tanggungjawabnya, selaras dengan keperluan pengasingan kerja. Ini bermakna seorang kakitangan dari operasi boleh mengaudit bahagian aplikasi dan sebaliknya, asalkan kakitangan itu tidak ditugaskan mengaudit bahagian dalam tanggungjawabnya sendiri.

b. Juru Audit Dalaman adalah dari SUK 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.

LAMPIRAN 1

BORANG AKUAN PEMATUHAN
DASAR KESELAMATAN ICT NEGERI MELAKA DAN
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

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 Dasar Keselamatan ICT Negeri Melaka dan ISMS; 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 : ……

LAMPIRAN 2

PENERANGAN BORANG-BORANG UNTUK PENTADBIRAN KESELAMATAN

Borang-borang yang digunakan dalam pentadbiran dan penguatkuasaan keselamatan ICT dilampirkan pada akhir dokumen ini. Aliran kegunaan borang-borang diterangkan dalam bahagian-bahagian yang berkaitan dalam dokumen ini manakala kegunaan borang-borang berkenaan diringkaskan dalam jadual berikut:

Borang	Nama Borang	Kegunaan	Kegunaan dan Tanggungjawab Mengisi Borang	Kelulusan Oleh	Pemantauan atau Semakan Oleh	Disahkan Oleh
A	Rekod Aset	Merekodkan aset-aset maklumat . Perhatian : Bagi aset-aset bukan maklumat, borang aset Kerajaan sedia ada boleh digunakan, tetapi maklumat tambahan yang perlu untuk setiap aset berkenaan hendaklah dicatitkan secara berasingan.	1. Untuk mengenalpasti aset, hubungkait aset dan juga mereka yang bertanggungjawab terhadap aset. 2. Setiap Jabatan perlu mengisi borang untuk aset di bawah kawalan masing-masing. 3. ICTSO perlu melakukan pelarasan: a. Tiada aset yang bertindih atau dalam bidangkuasa lebih dari satu Jabatan/ Agensi, dan b. Tiada aset yang tidak dikenalpasti pemiliknya atau pihak yang bertanggungjawab terhadap aset berkenaan sebagai Penjaga Aset.	Pegawai Keselamatan ICT Jabatan	Pegawai Keselamatan ICT Jabatan dicadangkan melakukan semakan dan kemaskini sekali setahun.	Tidak Perlu

Borang	Nama Borang	Kegunaan	Kegunaan dan Tanggungjawab Mengisi Borang	Kelulusan Oleh	Pemantauan atau Semakan Oleh	Disahkan Oleh
B	Fungsi-Fungsi Utama	Catitan fungsi-fungsi utama dan contoh tandatangan mereka yang bertanggungjawab dalam meluluskan, mengesahkan dan melaksanakan aktiviti pentadbiran dan penguatkuasaan keselamatan.	1. Borang-borang perlu diisi oleh kakitangan yang dikenalpasti dan ditugaskan dengan fungsi-fungsi tertentu dalam pentadbiran dan penguatkuasaan keselamatan. 2. Perlu dikemaskinikan oleh kakitangan yang terlibat apabila berlaku pertukaran.	Pegawai Keselamatan ICT Jabatan	Pegawai Keselamatan ICT dicadangkan melakukan semakan dan kemaskini sekali setahun.	Tidak Perlu
C	Permohonan Sistem/ Operasi ICT	Permohonan ID/ hak capaian dan/ atau perubahan aplikasi/ sistem oleh pengguna	1. ID dan hak capaian bagi pengguna baru. 2. Perubahan/ tambahan hak capaian bagi pengguna sediada. 3. Perubahan/ penambahan aplikasi/ sistem/ modul sedia ada.	Pemilik Aplikasi/ Sistem/ Data perlu luluskan.	Pemilik data dicadangkan melakukan semakan dan kemaskini sekali setahun.	Pegawai Keselamatan ICT Jabatan
D	Laporan Insiden/ Masalah	Laporan Insiden/ Masalah oleh pengguna kepada Khidmat Bantuan Tahap 1 Perhatian : Sistem laporan insiden/ masalah sedia ada	1. Pengguna mengisi butiran insiden/ masalah di Bahagian 1. 2. Khidmat Bantuan mengisi Bahagian 2 untuk mengesahkan dan menilaikan tahap insiden dan menyalurkan kepada pegawai tertentu untuk penyelesaian.	Tidak perlu	Pemantauan laporan yang tidak selesai oleh Khidmat Bantuan Tahap1 menerusi Borang E.	Khidmat Bantuan selepas masalah diselesaikan.

Borang	Nama Borang	Kegunaan	Kegunaan dan Tanggungjawab Mengisi Borang	Kelulusan Oleh	Pemantauan atau Semakan Oleh	Disahkan Oleh
		dalam Intranet perlu digunakan. Penerangan disini adalah untuk borang dan proses yang disediakan dalam dokumen ini . Jabatan/Agensi dikehendaki selaraskan amalannya dalam menggunakan sistem Intranet.	3. Pegawai yang ditugaskan menyelesaikan mengisi Bahagian 3. 4. Pegawai yang ditugaskan menyelesaikan mengisi Bahagian 4 sekiranya tidak dapat diselesaikan dan perlu Khidmat Bantuan Tahap 2 (mana yang berkenaan) 5. Pengguna mengesahkan masalah seselai di Bahagian 5. 6. Khidmat Bantuan Tahap 1 mengisi Bahagian 6 untuk menutup kes.			
E	Pemantauan dan Semakan Laporan Insiden/ Masalah	1. Pemantauan senarai laporan insiden/ masalah yang belum selesai. 2. Semakan senarai laporan dan jenis kerosakan	1. Pemantauan oleh Khidmat Bantuan Tahap 1 adalah untuk meninjau kemajuan penyelesaian insiden dan merangka tindakan untuk menyelesaikan. 2. Semakan dibuat selepas senarai insiden selesai, untuk merangka pelan pencegahan insiden jangka masa panjang supaya tidak berulang lagi.	Tidak perlu	1. Mana mana pegawai yang berkuasa atas Khidmat Bantuan. 2. Pegawai Keselamatan ICT atau wakilnya	Pengurusan ICT Jabatan

Borang	Nama Borang	Kegunaan	Kegunaan dan Tanggungjawab Mengisi Borang	Kelulusan Oleh	Pemantauan atau Semakan Oleh	Disahkan Oleh
F	Log Permohonan dan Penggunaan Superuser/ Root/ Admin ID	Untuk merekodkan permohonan dan sebab perlunya mengguna ID berkenaan	Kegunaan ID-ID ini perlu dikawal dan tidak harus digunakan selalu. Beberap ID-ID yang terhad fungsi dan kuasanya perlu ditubuhkan untuk kegunaan pentadbiran harian supaya ID Superuser/ Root/ Admin tidak perlu digunakan. Walaubagaimanapun keadaan tertentu mungkin memerlukan kegunaan ID tersebut.	Pegawai Keselamatan ICT	Pegawai Keselamatan ICT (audit log dari sistem perlu dijana oleh pemohon untuk bandingan dengan tindakan sebenar yang dicatitkan.)	Tidak perlu
G	Semakan Kegunaan ID Pentadbiran	Untuk merekodkan kegunaan ID-ID pentadbiran termasuk ID Pentadbir Aplikasi, ID Pentadbir Pangkalan Data dan ID Pentadbir Keselamatan	Guna borang berasingan untuk Pentadbiran Aplikasi, Pangkalan Data dan Keselamatan. Pentadbir berkenaan perlu mengisi borang dan kepilkan log aktiviti berkaitan untuk semakan.	Tidak perlu	Pegawai Keselamatan ICT (audit log dari sistem perlu dijana oleh pentadbir berkenaan untuk bandingan.)	Pegawai Keselamatan
H	Senarai Komponen Untuk Semakan	Untuk menyenaraikan komponen komponen selain daripada kegunaan ID-ID Pentadbiran	Senarai ini perlu dibincang oleh Jabatan untuk mengenalpasti komponen-komponen yang dianggap perlu disemak dari semasa ke semasa, siapa (fungsi) yang perlu menyemaknya dan kekerapan semakan.	Pegawai Keselamatan ICT Jabatan	Semakan dibuat jika perlu untuk menambah dan mengemaskini senarai komponen	Tidak perlu

Borang	Nama Borang	Kegunaan	Kegunaan dan Tanggungjawab Mengisi Borang	Kelulusan Oleh	Pemantauan atau Semakan Oleh	Disahkan Oleh
I	Semakan Jejak Audit	Ini serupa dengan Borang G tetapi untuk semakan senarai aktiviti komponen dalam Borang H.	Guna borang berasingan untuk tiap tiap komponen yang disenaraikan dalam Borang H. Borang diisi oleh fungsi yang bertanggungjawab terhadap komponen yang disemak aktivitinya.	Tidak Perlu	Fungsi yang ditugaskan (audit log dari sistem perlu dijana oleh fungsi berkenaan untuk semakan.)	Fungsi yang ditugaskan seperti di Borang H
J	Penamatan Akaun Aplikasi Dan Pemulangan Peralatan ICT	Digunakan untuk membatalkan ID login bagi akaun aplikasi/ sistem atau pemulangan peralatan ICT	Diisikan oleh pegawai/ kakitangan yang berpindah atau bersara. Pengurus/ Pemilik Aplikasi/ Sistem/ Data perlu mengambil tindakan dalam tempoh 14 hari dari tarikh akhir pegawai/ kakitangan tersebut berkhidmat	Tidak Perlu	Pengurus/ Pemilik Aplikasi/ Sistem/ Data	Pengurusan ICT Jabatan

Jadual 3: Penerangan Kegunaan Borang

BORANG A : Rekod Aset Aplikasi/Sistem

No Siri	

Jabatan : _____

Nama Aplikasi/Sistem : _____(senaraikan semua aplikasi/sistem dalam kawalan Jabatan)

No.	Nama Aset	Penge-nalan Aset	Penjaga Aset/ Pengguna Aset	Klasifikasi Aset (untuk maklumat atau data)	Lokasi Aset	Jangka Hayat Aset	Tahun / Harga Perolehan Aset	Hubungkait Aset	Penyelenggara Aset
1									
2									
3									
4									
5									
6									
7									

Di luluskan oleh Pegawai Keselamatan ICT Jabatan :

Tandatangan : _____

Nama : _____

Tarikh : _____

Perhatian : Borang sedia ada untuk merekod aset fizikal Kerajaan boleh digunakan tetapi hendaklah dicatitkan juga Penjaga Aset/Pengguna Aset, Jangka Hayat Aset, Harga Perolehan Aset dan Hubungkait Aset dengan Keselamatan ICT.

BORANG B : Fungsi Fungsi Utama
(dalam pentadbiran keselamatan ICT)

No Siri	

Jabatan : _____

Nama Aplikasi/Sistem : _____

Tarikh Kuatkuasa : _____

Fungsi (Tandakan Pilihan Dengan 'X') :

No.	Fungsi	Pilihan	Organisasi Pemilik (Untuk Pemilik Aplikasi/Sistem Sahaja)
1	Pemilik Aplikasi/Sistem		
2	Pengurus Aplikasi/Sistem		
3	Pemilik Data		
4	Pentadbir Aplikasi/Sistem		
5	Pentadbir Keselamatan		
6	Pentadbir Pangkalan Data		
7			<< Fungsi Lain – Sila Isi Nama Fungsi

Pegawai Utama (Primary)	Pegawai Gantian (Secondary)
Nama: _____	Nama: _____
Telefon: _____	Telefon: _____
Faks: _____	Faks: _____
Emel: _____	Emel: _____
T.Tangan :_____	T.Tangan :_____

Dengan ini, kandungan borang bernombor siri _____ bertarikh _____ dibatalkan.

Di perakui oleh Pegawai Keselamatan ICT Jabatan :

Tandatangan : _____

Nama : _____

Tarikh : _____

---------- **Catitan Kemaskini Rekod** ----------

Kandungan borang ini dibatalkan pada _____ dan diganti oleh borang bernombor siri _____ bertarikh _____.

BORANG C: Borang Permohonan/ Perubahan Sistem/ Operasi ICT

No Siri	

<table>
<tr><th colspan="3">MAKLUMAT PERMOHONAN</th></tr>
<tr><td colspan="2">NAMA :</td><td>NO.TELEFON :</td></tr>
<tr><td colspan="2">JAB./BAH./UNIT :</td><td>E-MEL :</td></tr>
<tr><td colspan="3">NAMA SISTEM/APLIKASI :</td></tr>
<tr><td colspan="2" rowspan="4">PERUBAHAN/PERMOHONAN YANG DIPERLUKAN:</td><td>TANDATANGAN PEMOHON:</td></tr>
<tr><td>TARIKH:</td></tr>
<tr><td>PENGESAHAN PENYELIA:</td></tr>
<tr><td>TARIKH:</td></tr>
<tr><th colspan="3">UNTUK KEGUNAAN PEJABAT SAHAJA</th></tr>
<tr><th colspan="3">KELULUSAN PEMILIK APLIKASI / SISTEM / DATA / KETUA UNIT</th></tr>
<tr><td colspan="2">JENIS :
[ ] Permohonan Baru [ ] Kemaskini Capaian
[ ] Penambahbaikan
[ ] Pertambahan Modul/ page baru</td><td>COP & TANDATANGAN :</td></tr>
<tr><td colspan="2">KEUTAMAAN : [ ] MINOR [ ] MAJOR [ ] KRITIKAL</td><td>TARIKH :</td></tr>
<tr><th colspan="3">TINDAKAN PEMBEKAL / PEMILIK APLIKASI / SISTEM / DATA</th></tr>
<tr><td colspan="2">DESKRIPSI PERUBAHAN YANG DILAKUKAN :</td><td rowspan="4">COP & TANDATANGAN :</td></tr>
<tr><td colspan="2">STATUS : [ ] SELESAI [ ] TANGGUH [ ] TOLAK</td></tr>
<tr><td>VERSI LAMA (jika ada):</td><td>VERSI BARU (jika ada):</td></tr>
<tr><td colspan="2">TARIKH :</td></tr>
<tr><th colspan="3">PENGESAHAN KETUA BAHAGIAN / UNIT</th></tr>
<tr><td colspan="2" rowspan="2">MAKLUMBALAS :</td><td>COP & TANDATANGAN :</td></tr>
<tr><td>TARIKH :</td></tr>
<tr><th colspan="3">PENGESAHAN PEMOHON</th></tr>
<tr><td colspan="2" rowspan="2">MAKLUMBALAS/ CATATAN:</td><td>TANDATANGAN :</td></tr>
<tr><td>TARIKH :</td></tr>
</table>

BORANG D: Laporan Insiden/ Masalah

No Siri	

(untuk diisi oleh Meja Bantuan)

Bahagian 1 : Untuk Diisi Oleh Pelapor Insiden/ Masalah

APLIKASI/ SISTEM ATAU PENGGUNAAN UMUM		
TARIKH LAPORAN		
TARIKH& WAKTUINSIDEN		
DILAPORKAN OLEH:		
	Nama dan Tandatangan	
	Jawatan	
	Jabatan/ Bahagian	
	Lokasi/ Alamat	
	No Telefon	
	No Faks	
	Emel	
	Alamat IP (Jika Diketahui dan berkaitan)	
BUTIR BUTIR APLIKASI/SISTEM (Jika Berkenaan atau Jika Diketahui)		
	Modul (Disyaki) Terlibat	
	Perkakasan (pelayan, komputer peribadi, switch, kebel dan sebagainya)	
	PengenalanPerkakasan Sekiranya Ada (Aset)	
PENERANGAN INSIDEN/MASALAH TERPERINCI (sertakan lampiran jika perlu)		

Bahagian 2 : Untuk Kegunaan Meja Khidmat Bantuan (Tahap 1)

Laporan Diterima Oleh			
Diterima Pada Tarikh/ Waktu			
Analisa Impak			
Tahap Kritikal (Bulatkan)	1. Tinggi	2. Sederhana	3. Rendah
Penyelasaian Masalah Ditugaskan Kepada			
Ditugaskan Pada Tarikh/ Waktu			

BORANG D : Laporan Insiden/Masalah

(sambungan)

No Siri	

(hendaklah sama dengan muka 1)

Bahagian 3 : Untuk Diisi Oleh Pegawai Yang Ditugaskan Menyelesaikan Insiden/Masalah Di Tahap 1

Tugas Penyelesaian Diterima Oleh	
Diterima Pada Tarikh/ Waktu	
Urutan Tindakan Yang Diambil dan Tarikh Tindakan. (Sila beri tarikh setiap tindakan sekiranya memakan masa beberapa hari)	1. 2. 3.
Masalah Diselesaikan (Ya/ Tidak)	
Tarikh Diselesaikan	

Bahagian 4 : Untuk Diisi Oleh Pegawai Yang Ditugaskan Menyelesaikan Insiden/Masalah Apabila Tidak Dapat Diselesaikan Di Tahap 1

Tarikh Insiden/ Masalah Dilaporkan Kepada Khidmat Bantuan Tahap 2 (Jika Berkenaan)	
Nama Pegawai Bertugas Tahap 2 Yang Menerima Laporan	
Urutan Tindakan Yang Diambil Di Tahap 2	Sila kepilkan laporan penyelesaian masalah Tahap 2 jika ada. Laporan ..... dikepilkan.
Masalah Diselesaikan (Ya/ Tidak)	
Tarikh Diselesaikan	

Bahagian 5 : Untuk Diisi Oleh Pelapor Masalah Selepas Masalah Diselesaikan

Penyelesaian Disahkan Oleh Pelapor Masalah atau Wakil :		
	Nama dan Tandatangan	
	Jawatan	
	Tarikh	

Bahagian 6 : Untuk Diisi Oleh Meja Khidmat Bantuan Tahap 1 Selepas Dilengkapkan Oleh Pelapor Masalah

Tarikh Terima Kembali Borang	

BORANG E : Pemantauan dan Semakan Penyelesaian Laporan Insiden/ Masalah

No Siri	

Jabatan : _____

Bil.	Tarikh Laporan	Nombor Siri Borang Insiden	Jenis Insiden	Tahap Kritikal	Ringkasan Langkah Penyelesaian	Tarikh Penyelesaian
1						
2						
3						
4						
5						
6						
7						
8						
9						

Pemantau (Pemantaun Berkala Untuk Menyelesaikan Insiden/ Masalah)

Nama	
Fungsi	
Tandatangan	
Tarikh-Tarikh Pemantauan	

Penyemak (Semakan Sekali Untuk Memastikan Corak Insiden/ Masalah Dan Menentukan Langkah Pencegahan Ulangan Insiden Jangka Masa Panjang)

Nama	
Fungsi	
Tandatangan	
Tarikh Semakan	

BORANG F : Log Permohonan dan Penggunaan Superuser/ Root/ Admin ID

No Siri	

Jabatan : _____

Nama Aplikasi/ Sistem : _____

No	Nama Pemohon Kegunaan ID	Tarikh	Sebab Permohonan (Ulaskan mengapa ID ini perlu digunakan dan bukan ID khusus dan terhad)	Diluluskan Oleh Pegawai Keselamatan ICT Jabatan	Perkara perkara yang ditukarkan atau dibetulkan	Ulasan (jika ada)	Sahkah Perubahan Berbanding Rekod Perubahan Dari Sistem?	Adakah Kata Laluan Diubah Selepas Digunakan?	Disemak oleh Pegawai Keselamatan ICT Setelah Pelaksanaan
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

BORANG G : Semakan Kegunaan ID Pentadbiran

No Siri	

Perhatian :

1. Borang ini adalah borang umum untuk memantau kegunaan ID pentadbiran untuk tiap tiap komponen Aplikasi, Pangkalan Data, Keselamatan, Alat Rangkaian, Alat Keselamatan (seperti Firewall dan IDS) dan sebagainya dan perlu dibandingkan dengan cetakan jejakan kegunaan dari log sistem atau perkakasan berkaitan. Satu borang ini perlu digunakan untuk satu komponen yang disemak.
2. Kerja kerja pentadbiran biasa atau berkala adalah dikecualikan dari direkod dalam borang ini.

Jabatan : _____

Nama Aplikasi/Sistem/Peralatan : _____

Komponen Yang Di Semak : _____

(Sila guna borang berasingan untuk tiap-taip komponen yang dipantau.)

Untuk Diisi Oleh Pentadbir Yang Melaksanakan					**Untuk Diisi Oleh Penyemak**
No	Nama Pentadbir	Capaian Komponen dari :		Rujukan Laporan Audit Jejak Kegunaan Yang Berkaitan	Tarikh Semakan
		Tarikh dan Waktu Mula	Tarikh dan Waktu Akhir		
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					

Tandatangan Penyemak (Pegawai Keselamatan ICT): _____

Nama : _____ Tarikh : _____

BORANG H : Senarai Komponen Semakan

No Siri	

Perhatian :

1. Borang ini adalah untuk merekod semua komponen yang telah ditetapkan dalam Jabatan untuk semakan atau pemantauan dan kekerapan pemantauan.

Jabatan : _____

Nama Aplikasi/ Sistem/ Peralatan : _____

No	Komponen Yang Dipantau/ Disemak	Bahan Yang Disemak	Pegawai bertanggungjawab Menjana Laporan Audit Trail (Jika berkenaan)	Pegawai bertanggungjawab Memantau/ Menyemak	Kekerapan Semakan (berapa bulan sekali?)
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Diperakui Oleh :

Pegawai Keselamatan ICT : _____

Nama : _____

Tarikh : _____

BORANG I : Semakan Audit Trail

No Siri	

Perhatian :

1. Borang ini adalah borang umum untuk memantau atau menyemak kegunaan aplikasi/sistem selain daripada kegunaan ID pentadbiran yang disemak berasingan melalui Borang H. Contoh pemantauan/semakan dalam Borang H ini adalah:
   a. Senarai kegunaan hak capaian untuk mengesan percubaan kegunaan yang melanggar hak yang diberikan (*access violations*) atau percubaan menggodam atau salahguna aplikasi/sistem.
   b. Senarai logon ID atau hak capaian berbanding dengan senarai yang dikemukakan oleh Ketua Jabatan pengguna setahun sekali.
   c. Urutan ubahan data utama dalam sistem (jika ada) berbanding dengan rujukan yang berasingan. Satu borang ini perlu digunakan untuk satu komponen yang dipantau.

Jabatan : _____

Nama Aplikasi/Sistem/Peralatan : _____

Komponen Yang Di Semak/Pantau : _____

(Sila guna satu borang untuk satu komponen yang dipantau atau disemak.)

No	Rujukan Laporan Audit Yang Berkaitan	Tarkih Laporan Audit	Log Audit Dari:		Disemak Oleh	Tarikh Semakan
			Tarikh Mula	Tarikh Akhir		
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						

Disahkan oleh :

Nama : _____

Jawatan : _____

Tarikh : _____

BORANG J : Penamatan Akaun Aplikasi Dan Pemulangan Peralatan

No Siri	

MAKLUMAT PEMOHON			
Nama:			
No. K.P:			
Jawatan & Gred:			
Jabatan/Bahagian:			
No.Telefon:		E-mel:	
Tarikh Tamat Perkhidmatan / Pertukaran:			
Sebab Penamatan:	☐ Tamat Perkhidmatan	☐ Pertukaran Dalaman	
	☐ Pertukaran ke Jabatan Negeri	☐ Pertukaran ke Jabatan Persekutuan/ Agensi	

PENGESAHAN KETUA JABATAN / PEMOHON

Dengan ini adalah disahkan bahawa maklumat yang diberikan di atas adalah benar.

Nama :
Jawatan :
Tarikh :

Tandatangan & Cop Rasmi

UNTUK KEGUNAAN PEJABAT

MAKLUMAT AKAUN APLIKASI/ SISTEM

Senarai Aplikasi/ Sistem	**Id**	**Dilaksanakan Oleh:**	**Tarikh:**
Domain & E-mel Rasmi			
Lain-lain, sila nyatakan:			
TINDAKAN	☐ Hapus	☐ Kemaskini	☐ Lain-lain _____

MAKLUMAT PERALATAN ICT

Senarai Peralatan ICT	**No. Rujukan:**	**Diterima Oleh:**	**Tarikh:**
Komputer			
Printer			
Lain-lain, sila nyatakan:			
TINDAKAN	☐ Hapus	☐ Kemaskini	☐ Lain-lain _____

Disemak/ Disahkan Oleh :

Tandatangan :
Tarikh :