# PROSEDUR KESELAMATAN ICT NEGERI MELAKA

**Versi 1.4 :: Julai 2014**

## KANDUNGAN

PENGENALAN DOKUMEN ..... iv
LOG KAWALAN KEMASKINI DOKUMEN ..... v
I. PENGENALAN ..... vii
II OBJEKTIF DOKUMEN ..... viii
III. HIERARKI DAN HUBUNGKAIT DOKUMEN ..... ix
IV. KATEGORI APLIKASI DAN SISTEM ..... x
V. PENERANGAN TERMINOLOGI FUNGSI ..... xiii
VI. PENERANGAN BORANG-BORANG UNTUK PENTADBIRAN KESELAMATAN ..... xvii
VII. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN ..... xxiii
VIII. PROSEDUR KESELAMATAN ICT NEGERI MELAKA ..... 1
Seksyen 1. Polisi Keselamatan Maklumat ..... 1
1.1. Tujuan Umum ..... 1
1.2. Prosedur Polisi Keselamatan Maklumat ..... 1
Seksyen 2. Pengurusan Keselamatan Maklumat ..... 1
2.1. Tujuan Umum ..... 1
2.2. Prosedur Pengurusan Keselamatan Maklumat ..... 1
Seksyen 3. Pengurusan Aset Berkaitan Maklumat ..... 4
3.1. Tujuan Umum ..... 4
3.2. Prosedur Pengurusan Aset ..... 4
Seksyen 4. Keselamatan Sumber Manusia ..... 6
4.1. Tujuan Umum ..... 6
4.2. Prosedur Keselamatan Sumber Manusia ..... 6
4.2.1. Tanggungjawab Kakitangan ..... 6
4.2.2. Penjawatan Kakitangan ..... 6
4.2.3. Latihan Kesedaran Keselamatan Maklumat ..... 6
4.2.4. Tanggungjawab kakitangan dan Tindakan Disiplin ..... 7
4.2.5. Pengendalian Kakitangan Yang Berpindah Atau Bersara ..... 7
4.2.6. Tindakbalas Kakitangan Terhadap Insiden Keselamatan ..... 8
Seksyen 5. Kawalan Fizikal dan Persekitaran ..... 9
5.1. Tujuan Umum ..... 9
5.2. Prosedur Kawalan Fizikal Dan Persekitaran ..... 9
5.2.1. Keperluan Umum ..... 9
Seksyen 6. Pengurusan Operasi dan Rangkaian ..... 11
6.1. Tujuan Umum ..... 11
6.2. Prosedur Pengurusan Operasi dan Rangkaian ..... 11
6.2.1. Pengurusan Konfigurasi ..... 11
6.2.1.1. Pengurusan Konfigurasi Perkakasan ..... 11
6.2.1.2. Pengurusan Konfigurasi Teknikal ..... 11

6.2.1.3. Perubahan Konfigurasi Sementara ..... 13
6.2.1.4. Perubahan Konfigurasi Dalam Keadaan Kecemasan ..... 14
6.2.2. Pengasingan Kerja ..... 15
6.2.3. Kawalan Kegunaan ID Yang Tinggi Hak Capaiannya ..... 15
6.2.4. Prosedur Kendalian (*Operating Procedures*) dan Dokumentasi ..... 17
6.2.5. Selenggaraan Aplikasi atau Sistem ..... 18
6.2.6. Perjanjian Tahap Perkhidmatan (SLA) ..... 18
6.2.7. Backup dan Media Backup ..... 19
6.2.8. Komputer Kerajaan Negeri ..... 19
6.2.9. Rangkaian Tanpa Wayar ..... 20
6.2.10. Perancangan Kapasiti Perkakasan ..... 21
6.2.11. Penggunaan Perisian *Anti-Virus* dan *Anti-Malware* ..... 22
6.2.12. Simpanan Rekod dan Pengurusan Kualiti ..... 23
6.2.13. Pemantauan Aktiviti Pelbagai ..... 23
Seksyen 7. Kawalan Capaian Logikal ..... 26
7.1. Tujuan Umum ..... 26
7.2. Prosedur Kawalan Capaian Logikal ..... 26
7.2.1. Kawalan Capaian Logikal Secara Umum ..... 26
7.2.2. Perlindungan Kata Laluan ..... 27
7.2.3. Pentadbiran ID dan Capaian Logikal ..... 27
7.2.4. Pemansuhan Hak Capaian Logikal ..... 27
7.2.5. Pemantauan Kegunaan Hak Capaian ..... 27
Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi ..... 29
8.1. Tujuan Umum ..... 29
8.2. Prosedur Pembangunan dan Penyelenggaraan Aplikasi ..... 29
8.2.1. Spesifikasi Keselamatan Dalam Aplikasi ..... 29
8.2.2. Pembangunan dan Penyelenggaraan Aplikasi ..... 30
Seksyen 9. Pengurusan Insiden ..... 32
9.1. Tujuan Umum ..... 32
9.2. Prosedur Pengurusan Insiden ..... 32
9.2.1. Laporan Insiden dan Penyelesaian ..... 32
9.2.2. Pemantauan Penyelesaian Laporan Insiden ..... 33
Seksyen 10. Pengurusan Kesinambungan Perkhidmatan ..... 36
10.1. Tujuan Umum ..... 36
10.2. Prosedur Pengurusan Kesinambungan Perkhidmatan ..... 36
10.2.1. Kewajipan Merangka Kesinambungan Perkhidmatan ..... 36
10.2.2. Analisa Dan Mengenalpasti Perkhidmatan Penting ..... 36
10.2.3. Perlaksanaan Pelan dan Ujian ..... 37
Seksyen 11. Pematuhan ..... 38
11.1. Tujuan Prosedur ..... 38
11.2. Prosedur Pematuhan ..... 38
11.2.1. Pematuhan Kepada Keperluan Undang Undang ..... 38

11.2.2. Semakan Polisi Keselamatan Dan Pematuhan ..... 38
11.2.3. Keperluan Audit ..... 39
11.2.4. Audit Dalaman dan Luaran ..... 39
11.2.5. Hak Capaian Untuk Juru Audit ..... 40
DEFINISI POLISI, STANDARD, GARIS PANDUAN DAN PROSEDUR ..... 41
KEMBARAN : BORANG BORANG BERKAITAN PENTADBIRAN KESELAMATAN 43
BORANG A : Rekod Aset Aplikasi/Sistem ..... 1
BORANG B : Fungsi Fungsi Utama ..... 2
BORANG C : Borang Permohonan Sistem / Operasi ICT ..... 3
BORANG D : Laporan Insiden/Masalah ..... 4
BORANG E : Pemantauan dan Semakan Penyelesaian Laporan Insiden/Masalah .... 6
BORANG F : Log Permohonan dan Penggunaan Superuser/Root/Admin ID ..... 7
BORANG G : Semakan Kegunaan ID Pentadbiran ..... 8
BORANG H : Senarai Komponen Semakan ..... 9
BORANG I : Semakan Audit Trail ..... 10

Rajah 1 : Proses Merekod Fungsi Utama ..... 2
Rajah 2 : Proses Merekod Aset ..... 5
Rajah 3 : Proses Kegunaan ID Pentadbir ..... 12
Rajah 4 : Proses Kegunaan ID Superuser/Root/Admin ..... 17
Rajah 5 : Proses Permohonan Rangkaian Tanpa Wayar ..... 21
Rajah 6 : Proses Merekod Senarai Komponen Untuk Semakan ..... 24
Rajah 7 : Proses Semakan Komponen ..... 25
Rajah 8 : Proses Permohonan ID/Hak Capaian dan/atau Perubahan Aplikasi/Sistem ..... 26
Rajah 9 : Proses Laporan Insiden dan Penyelesaian Insiden ..... 33
Rajah 10 : Proses Pemantauan Penyelesaian Insiden ..... 34
Rajah 11 : Proses Semakan Laporan Insiden ..... 35

## PENGENALAN DOKUMEN

| | |
|---|---|
| **NAMA DOKUMEN:** | **Prosedur Keselamatan ICT Negeri Melaka** |
| **VERSI:** | **1.4** |
| **TARIKH:** | **Julai 2014** |

## LOG KAWALAN KEMASKINI DOKUMEN

| No. | 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 | 6.2.9 Rangkaian Tanpa Wayar | Tambahan perenggan di para 6.2.9 (a) |
| 3 | 5/6/2012 | Semua | Pindaan perkataan rakam kepada rekod |
| | | I. Pengenalan | Tambahan perenggan di mukasurat vii |
| | | IV. Kategori Aplikasi dan Sistem | Menggugurkan perenggan di mukasurat xii |
| | | XI.Penerangan Terminologi Fungsi | Pindaan fungsi Jawatankuasa<br>Tambahan fungsi Ketua Pegawai Maklumat (CIO). |
| | | VI. Penerangan Borang-Borang Untuk Pentadbiran Keselamatan | Pindaan Nama, Kegunaan dan Tanggungjawab dan Disahkan Oleh pada Borang C |
| | | X.Pengemaskinian Dan Penyenggaraan Dokumen | Pindaan Jawatankuasa<br>Pindaan No.Telefon<br>Tambahan keterangan * |
| | | Seksyen 4. Keselamatan Sumber Manusia | Pindaan Pengurus/Pemilik di para 4.2.5 |
| | | Seksyen 9. Pengurusan Insiden | Tambahan proses laporan di para 9.2.1<br>Pindaan proses pemantauan di para 9.2.2 |
| | | Kembaran : Borang Borang Berkaitan Pentadbiran Keselamatan | Pindaan pilihan di Borang B<br>Pindaan Keseluruhan Borang C |

| No. | Tarikh | Bahagian Yang Berkenaan | Keterangan Perubahan |
|---|---|---|---|
| 4 | 23 Julai 2014 | IV. KATEGORI APLIKASI DAN SISTEM | • Pindaan Jadual 1:<br>○ E-ADUAN kepada Sistem Pengurusan Aduan Bersepadu Kerajaan Negeri Melaka (SISPAA)<br>○ Portal EPG kepada Gerbang Pembayaran Bersepadu Kerajaan Negeri Melaka (e-Bayar)<br>• Menggugurkan *Generic Office Environment* – Electronic *Government Document Management System* (GOE-EGDMS) dari Jadual 1 |
| | | VII. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN | • Pindaan Bahagian Perkhidmatan Teknologi Maklumat kepada Bahagian Teknologi Maklumat dan Komunikasi (BTMK)<br>• Pindaan BPTM kepada BTMK<br>• Pindaan Pengarah kepada Ketua ICT Negeri |
| | | Seksyen 4. Keselamatan Sumber Manusia | • Pindaan BPTM kepada BTMK di para 4.2.3.a<br>• Pembetulan ayat di para 4.2.6.c. : masalah yang dilaporkan |
| | | Seksyen 6. Pengurusan Operasi dan Rangkaian | • Pindaan BPTM kepada BTMK di para 6.2.8.c dan 6.2.11.a |

# I. PENGENALAN

Dokumen ini, Prosedur Keselamatan ICT Negeri Melaka (Prosedur) menggariskan **prosedur umum untuk kegunaan** di semua Jabatan Kerajaan Negeri Melaka (Kerajaan Negeri). Walau bagaimanapun, jabatan/agensi boleh menggunapakai prosedur masing-masing mengikut kesesuaian.

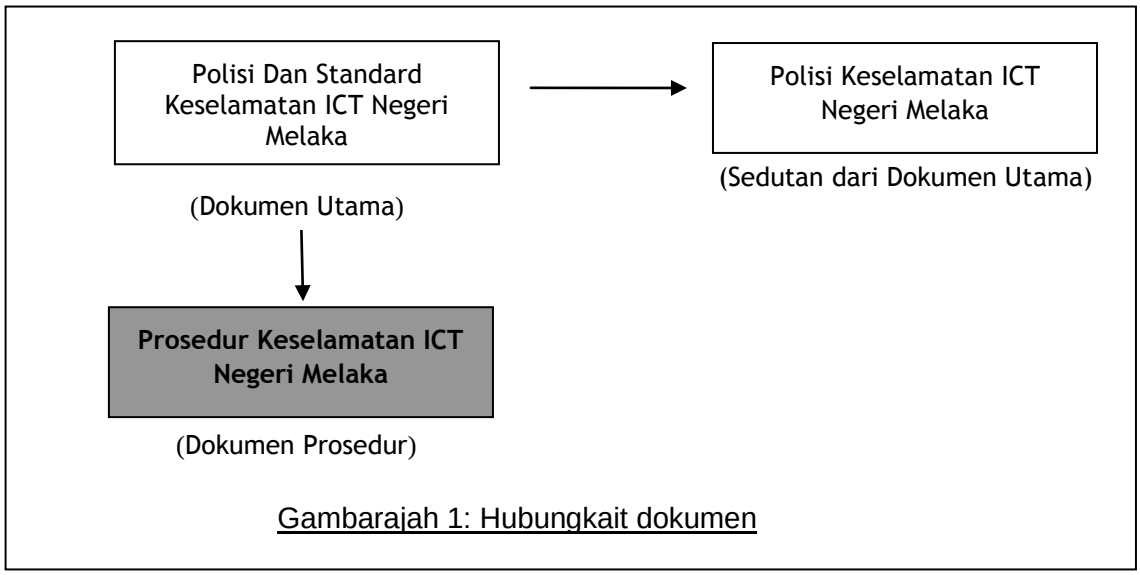
## II. OBJEKTIF DOKUMEN

Objektif dokumen prosedur ini adalah:

1. Menyediakan prosedur minimum untuk pentadbiran dan penguatkuassan keselamatan ICT;
2. Menyediakan panduan perlaksanaan, pematuhan, pemantauan dan semakan untuk menentukan amalan yang konsisten dan mudah dikawal;
3. Menyediakan langkah-langkah bagi melaporkan dan menyelesaikan insiden atau masalah;
4. Menyediakan panduan antaramuka semua yang terlibat dalam pentadbiran keselamatan ICT; dan
5. Menerangkan panduan penggunaan Borang-Borang untuk memudahkan pentadbiran dan penguatkuasaan keselamatan ICT.

## III. HIERARKI DAN HUBUNGKAIT DOKUMEN

Dokumen Prosedur Keselamatan ICT ini adalah sedutan dari dokumen utama untuk tujuan rujukan. Prosedur Keselamatan ICT Negeri Melaka ini merupakan langkah-langkah terperinci yang dibangunkan bagi menyokong pelaksanaan Polisi dan Standard Keselamatan ICT Negeri Melaka. Hubungkait keseluruhan dokumen adalah seperti Gambarajah 1:




Gambarajah 1: Hubungkait dokumen

## IV. KATEGORI APLIKASI DAN SISTEM

Beberapa aplikasi dan sistem telah dibangunkan dan digunapakai oleh Jabatan Kerajaan Negeri. Di samping itu, ada 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/emel |
| 2 | Portal Rasmi Kerajaan Negeri Melaka | Semua Jabatan | Penyebaran maklumat dan interaksi antara rakyat dan Kerajaan Negeri Melaka |
| 3 | e-DUN | Semua Jabatan | Urusan persidangan soal jawab Dewan Undangan Negeri |
| 4 | e-MMKN | Semua Jabatan | Penyediaan dan penyaluran kertas risalat Majlis Mesyuarat Kerajaan Negeri |
| 5 | Sistem Pendaftaran Tanah Berkomputer (SPTB), Land Revenue Information System (LaRIS) | Pejabat Daerah dan Tanah, Pejabat Pengarah Tanah dan Galian | Urusan tanah dan percukaian |
| 6 | Sistem Pengurusan Aduan Bersepadu Kerajaan Negeri | Semua Jabatan | Terimaan dan aturan tindakan susulan terhadap aduan dan |

| Bil. | Sistem atau Aplikasi Penting dan Kritikal | Kegunaan | Proses Yang Disokong |
|---|---|---|---|
| | Melaka (SISPAA) | | pertanyaan dari orang ramai menerusi portal |
| 7 | Kawalan Keselamatan Akses Pintu | Semua Jabatan (Seri Negeri) | Kawalan akses fizikal di Seri Negeri |
| 8 | Sistem Perakaunan dan Kewangan Standard - SPEKS | Semua Jabatan | Pentadbiran kewangan, akaun dan pembayaran secara elektronik |
| 9 | Gerbang Pembayaran Bersepadu Kerajaan Negeri Melaka (e-Bayar) | Lembaga Perumahan (e-SPARA), Perbadanan Ketua Menteri (e-ProMIS), Bendahari Negeri (SPEKS), Tabung Amanah Pendidikan Negeri Melaka (e-TAPEM), Majlis Perbandaran Hang Tuah Jaya (MPHTJ.Net), Majlis Perbandaran Jasin (ePBT), Majlis Perbandaran Alor Gajah (AVIS) | Terimaan bayaran secara elektronik dari orang awam |
| 10 | Sistem Penganugerahan Darjah Kebesaran Negeri Melaka | Jabatan Ketua Menteri | Urusan penganugerahan dan catitan latar belakang penerima pingat |
| 11 | Emel dan Kalendar Rasmi Kerajaan Negeri Melaka | Semua Jabatan | Emel dan kalendar |
| 12 | e-TAPEM | Tabung Amanah Pendidikan | Urusan bantuan dan pinjaman pelajaran anak Negeri Melaka |
| 13 | e-SPARA | Lembaga Perumahan, Pejabat Daerah dan Tanah | Pentadbiran akaun rumah awam/pangsa dan pemantauan |
| 14 | *Human Resource Management Information System* (HRMIS) | Semua Jabatan | Pentadbiran sumber manusia |
| 15 | Sistem Permohonan Kebenaran Pindah milik dan Gadaian (e-Consent) | Pejabat Daerah dan Tanah, Pejabat Pengarah Tanah dan Galian | Urusan permohonan kebenaran pindah milik dan gadaian. |

| Bil. | Sistem atau Aplikasi Penting dan Kritikal | Kegunaan | Proses Yang Disokong |
|---|---|---|---|
| 16 | *Malaysian Geospatial Data Infrastructure* (MyGDI) | Semua jabatan yang terlibat dalam pengurusan Data Geospatial | Platform bagi memudahkan capaian dan perkongsian maklumat geospatial antara agensi. |
| 17 | *Sistem e-Syariah* | Mahkamah Syariah Negeri Melaka | Mempertingkatkan kualiti pentadbiran Institusi Kehakiman dalam pengurusan kes mahkamah Syariah |

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

## V. PENERANGAN TERMINOLOGI FUNGSI

Bahagian ini menerangkan terminologi fungsi yang digunakan dalam dokumen ini. Bidang tugas fungsi secara terperinci diterangkan dalam dokumen Polisi dan Standard Keselamatan ICT Negeri Melaka tetapi fungsi utama diringkaskan dibawah ini supaya senang dirujuk:

| No. | Nama Fungsi | Penerangan Bidang Tugas |
|---|---|---|
| 1 | Juru Audit Dalaman | Juru Audit daripada SUK yang membuat audit dalaman berkaitan pematuhan polisi keselamatan ICT. |
| 2 | Juru Audit Jabatan | Kakitangan Jabatan yang ditugaskan untuk menjalankan audit pemantauan dalam Jabatan sendiri, dari masa ke semasa sebagai tugas sampingan. |
| 3 | Juru Audit Luaran | Juru Audit daripada kalangan pakar atau perunding yang boleh membuat audit teknikal berkaitan pematuhan polisi keselamatan ICT. |
| 4 | Jawatankuasa Pemandu Teknologi Maklumat Negeri Melaka | Jawatankuasa ini menentukan hala tuju pelaksanaan ICT Negeri Melaka, menetapkan polisi keselamatan ICT dan memantau tahap perlaksanaan dan serta pematuhan polisi oleh semua kakitangan Kerajaan Negeri Melaka. |
| 5 | Ketua Jabatan/Pegawai Pengawal | Pegawai yang menyokong atau mengesahkan permohonan ID dan hak capaian pengguna dalam Jabatan 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. |
| 6 | Khidmat Bantuan Tahap 1 | Bantuan dari Jabatan sendiri dalam penyelesaian masalah atau insiden dalam Jabatan. |

| No. | Nama Fungsi | Penerangan Bidang Tugas |
|---|---|---|
| 7 | Khidmat Bantuan Tahap 2 | Bantuan dari pihak yang membekalkan aplikasi atau sistem dibawah pengurusan Pemilik Aplikasi atau Sistem. |
| 8 | Pemilik Aset | Ketua Jabatan yang bertanggungjawab terhadap pemilikan aset bagi pihak Kerajaan. |
| 9 | Pemilik Aplikasi/Sistem | Pemilik Aplikasi atau Sistem adalah untuk aplikasi atau sistem yang dibekalkan dan masih dalam tanggungjawab selenggaraan 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 Sistem Pendaftaran Tanah Berkomputer atau SPTB. |
| 10 | Penjaga atau Pengguna Aset | Kakitangan yang bertanggungjawab terhadap kesiapsediaan aset atau keselamatan aset untuk kegunaan harian. |
| 11 | Pemilik Data | Pemilik Data bertanggungjawab meluluskan permohonan hak capaian kepada data/bahagian aplikasi yang diperlukan pengguna. **Perhatian:** Sesebuah aplikasi (terutama sekali aplikasi yang besar), boleh ada beberapa Pemilik Data yang masing masing berkuasa dan bertanggungjawab atas bahagian data bawah tadbiran atau kawalannya. |
| 12 | Pengguna-Pengguna | Pengguna-pengguna aplikasi. |
| 13 | Pengurus Aplikasi/Sistem | Pengurus Aplikasi atau Sistem adalah untuk aplikasi atau sistem yang dibangunkan dalam Jabatan atau dimilik, ditadbir dan disokong (*support*) sepenuhnya oleh Jabatan. Segala rancangan naiktaraf dan pembetulan fungsi aplikasi/sistem diaturkan oleh Pengurus Aplikasi atau |

| No. | Nama Fungsi | Penerangan Bidang Tugas |
|---|---|---|
| | | Sistem. |
| 14 | Ketua Pegawai Maklumat (CIO) | Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju ICT Negeri Melaka. |
| 15 | Pegawai Keselamatan ICT (atau ICTSO Jabatan) | Pegawai Keselamatan ICT Jabatan bertanggungjawab keseluruhan untuk memastikan Jabatannya mematuhi Polisi Keselamatan ICT Negeri Melaka. Sekiranya Jabatan memerlukan pengecualian (sementara atau tetap) dalam pematuhan Polisi Keselamatan, maka beliau bertanggungjawab menilai keperluan dan implikasi pengecualian, dan mendokumenkan pengecualian tersebut. |
| 16 | Pentadbir Aplikasi/Sistem | Pentadbir Aplikasi/Sistem adalah fungsi teknikal yang bertanggungjawab menentukan bahawa aplikasi berjalan dengan baik. Antara tugas beliau ialah melaksanakan konfigurasi aplikasi, peruntukkan sumber CPU dan memori (*CPU and memory resources*), melaksanakan 'patches' dan naiktaraf (*upgrade*), menjana log aktiviti dan membersihkan log. |
| 17 | Pentadbir Pangkalan Data | Pentadbir Pangkalan Data adalah fungsi teknikal yang bertanggungjawab menentukan bahawa pangkalan data berfungsi dengan baik dan dikemaskini dari masa ke semasa. Antara tugas beliau ialah melaksanakan perubahan pangkalan data sekiranya diarahkan oleh pembekal sistem, menjana log, membersihkan log, re-indexing. |
| 18 | Pentadbir Keselamatan | Pentadbir Keselamatan bertanggungjawab melaksanakan permohonan hak capaian pengguna yang telah diluluskan oleh Pemilik Data. Perhatian : Pentadbir Keselamatan boleh |

| No. | Nama Fungsi | Penerangan Bidang Tugas |
|---|---|---|
| | | mentadbirkan keselamatan untuk lebih dari satu aplikasi atau sistem. |
| 19 | Penyelaras Prosidur | Pegawai yang bertanggungjawab mengemaskini dan menyebarkan prosidur-prosidur berkaitan kegunaan, pengurusan dan selenggaraan aplikasi atau perkhidmatan sokongan. |

Jadual 2: Terminologi Fungsi dan Bidang Tugas

## VI. PENERANGAN BORANG-BORANG UNTUK PENTADBIRAN KESELAMATAN

Borang-borang yang digunakan dalam pentadbiran dan penguatkuasaan keselamatan ICT dilampirkan di Kembaran 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 .<br><br>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.<br>2. Setiap Jabatan perlu mengisi borang untuk aset di bawah kawalan masing-masing.<br>3. ICTSO perlu melakukan pelarasan:<br>a. Tiada aset yang bertindih atau dalam bidangkuasa lebih dari satu Jabatan, dan<br>b. Tiada aset yang tidak | 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 |
|---|---|---|---|---|---|---|
| | | | dikenalpasti pemiliknya atau pihak yang bertanggungjawab terhadap aset berkenaan sebagai Penjaga Aset. | | | |
| 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.<br>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.<br>2. Perubahan/tambahan hak capaian bagi pengguna sediada.<br>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 |

| Borang | Nama Borang | Kegunaan | Kegunaan dan Tanggungjawab Mengisi Borang | Kelulusan Oleh | Pemantauan atau Semakan Oleh | Disahkan Oleh |
|---|---|---|---|---|---|---|
| D | Laporan Insiden/Masalah | Laporan Insiden/Masalah oleh pengguna kepada Khidmat Bantuan Tahap 1<br><br>Perhatian : Sistem laporan insiden/masalah sedia ada dalam Intranet perlu digunakan.<br>Penerangan disini adalah<br>untuk borang dan proses yang disediakan dalam dokumen ini . Jabatan jabatan dikehendaki selaraskan amalannya dalam menggunakan sistem Intranet. | 1. Pengguna mengisi butiran insiden/masalah di Bahagian 1.<br>2. Khidmat Bantuan mengisi Bahagian 2 untuk mengesahkan dan menilaikan tahap insiden dan menyalurkan kepada pegawai tertentu untuk penyelesaian.<br>3. Pegawai yang ditugaskan menyelesaikan mengisi Bahagian 3.<br>4. Pegawai yang ditugaskan menyelesaikan mengisi Bahagian 4 sekiranya tidak dapat diselesaikan dan perlu Khidmat Bantuan Tahap 2 (mana yang berkenaan)<br>5. Pengguna mengesahkan masalah seselai di Bahagian 5. | 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 |
|---|---|---|---|---|---|---|
| | | | 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.<br>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.<br>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.<br>2. Pegawai Keselamatan ICT atau wakilnya | Pengurusan ICT Jabatan |
| 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 | Pegawai Keselamatan ICT | Pegawai Keselamatan ICT (audit log dari sistem perlu dijana oleh pemohon untuk | Tidak perlu |

| Borang | Nama Borang | Kegunaan | Kegunaan dan Tanggungjawab Mengisi Borang | Kelulusan Oleh | Pemantauan atau Semakan Oleh | Disahkan Oleh |
|---|---|---|---|---|---|---|
| | | | digunakan. Walaubagaimanapun keadaan tertentu mungkin memerlukan kegunaan ID tersebut. | | bandingan dengan tindakan sebenar yang dicatitkan.) | |
| 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 di semak dari masa 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 |
| I | Semakan Jejak | Ini serupa dengan Borang | Guna borang berasingan untuk tiap | Tidak Perlu | Fungsi yang | Fungsi yang |

| Borang | Nama Borang | Kegunaan | Kegunaan dan Tanggungjawab Mengisi Borang | Kelulusan Oleh | Pemantauan atau Semakan Oleh | Disahkan Oleh |
|---|---|---|---|---|---|---|
| | Audit | G tetapi untuk semakan senarai aktiviti komponen dalam Borang H. | tiap komponen yang disenaraikan dalam Borang H.<br>Borang diisi oleh fungsi yang bertanggungjawab terhadap komponen yang disemak aktivitinya. | | ditugaskan (audit log dari sistem perlu dijana oleh fungsi berkenaan untuk semakan.) | ditugaskan seperti di Borang H |

Jadual 3: Penerangan Kegunaan Borang

## VII. PENGEMASKINIAN DAN PENYENGGARAAN DOKUMEN

Dokumen ini adalah tertakluk kepada kawalan (*controlled document*) di mana segala perubahan hendaklah 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 lain tidak dibenarkan mengubah dokumen ini. Sebarang permintaan dan cadangan pengubahsuaian atau perubahan hendaklah dihantar kepada BTMK di alamat:

| | | |
|---|---|---|
| Nama | : | Ketua ICT Negeri,<br>Bahagian Teknologi Maklumat dan Komunikasi |
| Alamat | : | Aras 1, Blok Temenggong,<br>Seri Negeri, Hang Tuah Jaya,<br>Ayer Keroh,<br>75450 Melaka |
| Telefon | : | 06-333 3333 |
| Faksimili | : | 06-232 8620 |
| E-mel | : | <pengarahict>*@melaka.gov.my |

* <pengarahict> tertakluk kepada pengarah BTMK semasa

# VIII. PROSEDUR KESELAMATAN ICT NEGERI MELAKA

## Seksyen 1. Polisi Keselamatan Maklumat

### 1.1. Tujuan Umum

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 kitarhayat maklumat dan kemudahan pemprosesan maklumat dalam kawalan Jabatan.

### 1.2. Prosedur Polisi 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 perlaksanaan dan pematuhan prosedur keselamatan,
   iii. Tindakan pencegahan (*preventive action*),
   iv. Tindakan pembetulan (*corrective action*),
   v. Aktiviti audit dan pematuhan,
   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 Umum

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

### 2.2. Prosedur Pengurusan Keselamatan Maklumat

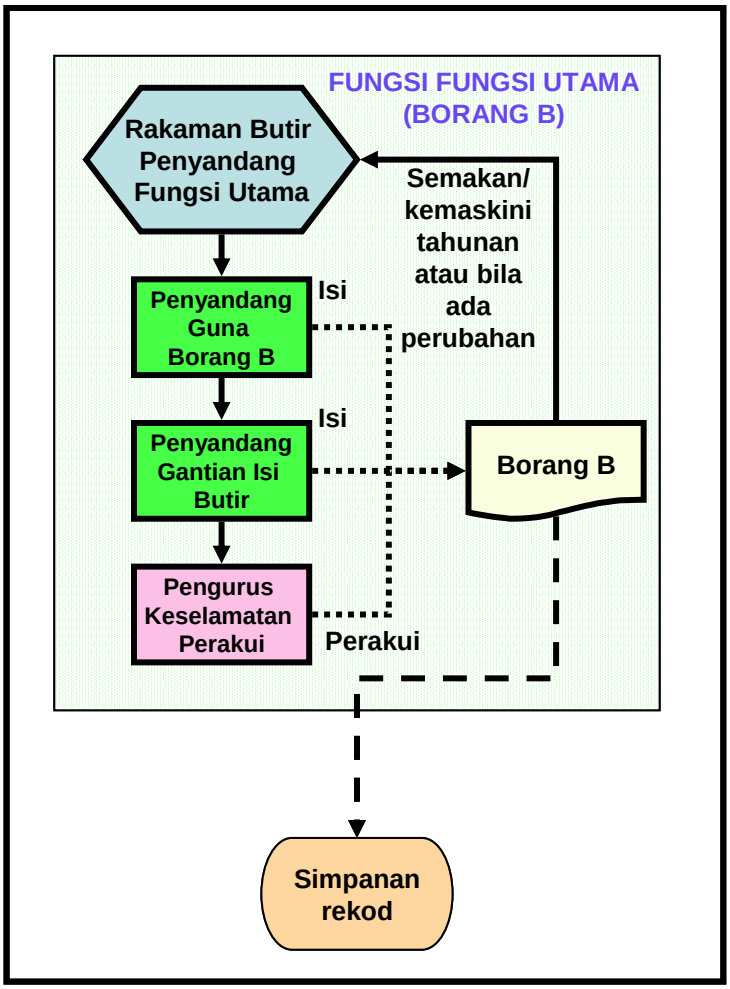
a. Pegawai Keselamatan ICT Jabatan hendaklah mengenalpasti pegawai-pegawai yang akan memegang berbagai fungsi seperti diterangkan di dalam Dokumen Polisi dan Standard Keselamatan ICT Negeri Melaka.

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

c. Perlaksanaan dan penguatkuasaan keselamatan ICT hendaklah dibuktikan dengan dokumen dan rekod yang berkaitan. Borang A hingga I dalam bahagian Kembaran dan telah diterangkan dalam seksyen VI, wajib 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 I dan lain-lain borang khusus yang digunakan.

e. Pegawai yang menyandang atau dilantik memegang fungsi kritikal dalam pengurusan dan pentadbiran keselamatan hendaklah direkodkan dalam Borang B mengikut proses dalam Rajah 1:




Rajah 1 : Proses Merekod Fungsi Utama

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 dicatitkan di sebelah bawah Borang B.

iv. Pegawai Keselamatan ICT perlu mengesahkan penamaan dan butiran dalam Borang B.

g. Pentauliahan Pegawai Keselamatan ICT boleh dibuat menerusi Borang B

tetapi pengesahan butirannya hendaklah dilakukan oleh pengurusan yang lebih tinggi. Pentauliahan Pegawai Keselamatan ICT boleh juga dibuat menerusi surat lantikan dari pengurusan atasan.

h. Tempat simpanan rekod hendaklah dikenalpasti, dan semua borang yang telah diisi serta dokumen sokongannya hendaklah disimpan di tempat simpanan rekod.

i. Jabatan bebas memilih tempat simpanan rekod masing-masing. Walaubagaimanapun, tempat simpanan rekod itu hendaklah dicatitkan. 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.

## Seksyen 3. Pengurusan Aset Berkaitan Maklumat

### 3.1. Tujuan Umum

Tujuan prosedur ini adalah untuk merekod semua aset yang berkaitan dengan pentadbiran, pengurusan dan keselamatan ICT, supaya perlindungan dan kawalan yang sewajarnya dapat dilaksanakan untuk semua proses kerja yang berkaitan.

### 3.2. Prosedur Pengurusan Aset

a. Semua aset fizikal Jabatan yang berkaitan dengan perjalanan sistem maklumat (termasuk aset sokongan seperti penghawa dingin bilik pelayan), 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 (dan aset yang tidak direkodkan dalam borang aset Kerajaan sedia ada) hendaklah direkodkan dalam Borang A dengan butir-butir berkaitan termasuk:

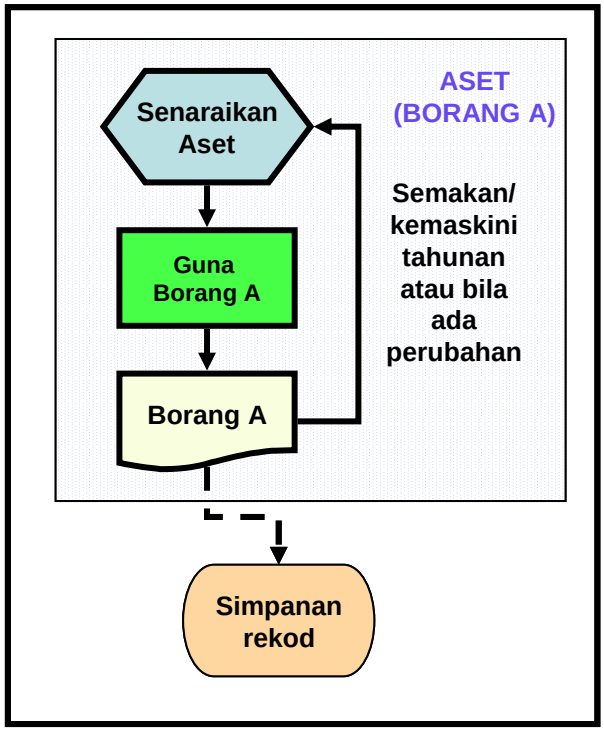
   i. Pemilik Aset (*asset owner*),
   ii. Penjaga Aset atau Pengguna Aset (*asset custodian*),
   iii. Klasifikasi aset (untuk aset maklumat atau data),
   iv. Lokasi aset,
   v. Jangka hayat aset (sekiranya maklumat ini ada),

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 mengguna Borang A ditunjukkan dalam Rajah 2:




Rajah 2 : Proses Merekod Aset

d. Senarai aset hendaklah dikemaskini sekurang-kurangnya sekali setahun atau apabila perubahan berlaku.

e. Semua kakitangan hendaklah mengendalikan aset mengikut Standard yang telah ditetapkan dalam Dokumen Polisi dan Standard Keselamatan ICT Negeri Melaka.

## Seksyen 4. Keselamatan Sumber Manusia

### 4.1. Tujuan Umum

Tujuan prosedur ini adalah untuk memastikan bahawa sumber manusia diambil kira dalam perlaksanaan Polisi dan Standard keselamatan ICT.

### 4.2. Prosedur Keselamatan Sumber Manusia

#### 4.2.1. Tanggungjawab Kakitangan

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

#### 4.2.2. Penjawatan Kakitangan

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

#### 4.2.3. Latihan Kesedaran Keselamatan Maklumat

a. Jadual latihan hendaklah disediakan setiap tahun oleh BTMK dan ICT Jabatan-Jabatan dan diaturkan supaya semua kakitangan diberi peluang untuk hadir sekurang-kurangnya sekali setahun.

b. Bahan latihan yang seragam hendaklah disediakan untuk tujuan latihan kesedaran keselamatan maklumat.

c. Latihan ini hendaklah memetik contoh-contoh amalan atau insiden yang pernah berlaku sama ada dalam Jabatan, Kerajaan Negeri atau di luar.

d. Semua pengguna hendaklah menandatangani kehadiran mereka dalam latihan.

e. Meja Khidmat Bantuan hendaklah memberi penerangan ringkas berkaitan Polisi, Standard dan Prosedur kepada pengguna baru sekiranya tarikh latihan yang ditetapkan masih jauh.

### 4.2.4. Tanggungjawab kakitangan dan Tindakan Disiplin

a. Semua kakitangan hendaklah mengambil maklum tanggungjawab mereka terhadap keselamatan maklumat dan akibatnya kepada Kerajaan Negeri sekiranya keselamatan maklumat tidak dikawal.

b. Kakitangan hendaklah menghadiri latihan dan taklimat keselamatan maklumat yang dianjurkan dari masa ke semasa dan memperakui kefahaman mereka berkenaan:

- Tanggungjawab dalam memastikan kerahsiaan maklumat,
- Tanggunjawab membantu dan memperingatkan rakan sepejabat serta pelawat-pelawat berkaitan polisi dan standard keselamatan yang perlu dipatuhi.
- Tanggungjawab melaporkan pelanggaran polisi atau ketidakpatuhan terhadap keselamatan pengendalian maklumat atau keselamatan fizikal, walaupun hanya disyaki,
- Kefahaman tindakan disiplin boleh diambil terhadap mereka sekiranya tidak mematuhi polisi keselamatan.

### 4.2.5. Pengendalian Kakitangan Yang Berpindah Atau Bersara

a. Ketua Jabatan bagi kakitangan yang berpindah atau bersara hendaklah memaklumkan kepada Pengurus/Pemilik Aplikasi/Sistem/Data mengenai perubahan tersebut dan memastikan bahawa Borang C untuk permohonan Logon ID dan hak capaian untuk kakitangan pengganti dikemukakan.

### 4.2.6. Tindakbalas Kakitangan Terhadap Insiden Keselamatan

a. Sekiranya kakitangan mengalami insiden keselamatan sama ada dalam bentuk pencerobohan, gangguan fungsi sistem, kelembapan sistem, serangan virus dan lain-lain hendaklah memantau keadaan dan melaporkan dengan segera kepada Khidmat Bantuan Tahap 1 dengan menggunakan Borang D.

b. Jika laporan dibuat melalui telefon atau emel, maka kakitangan tersebut hendaklah menyusulinya dengan Borang D yang telah diisi.

c. Kakitangan hendaklah memantau perkembangan penyelesaian insiden atau masalah yang dilaporkan dan berhubung dengan meja Khidmat Bantuan untuk mengetahui tindakan yang akan diambil.

d. Kakitangan hendaklah memberi kerjasama sepenuhnya untuk membantu penyiasatan dan penyelesaian masalah atau insiden yang dihadapi.

e. Kakitangan hendaklah mengesahkan penyelesaian masalah di Bahagian 5 Borang D dan kembalikan borang tersebut kepada meja Khidmat Bantuan dengan segera.

## Seksyen 5. Kawalan Fizikal dan Persekitaran

### 5.1. Tujuan Umum

Prosedur 'Kawalan Fizikal dan Persekitaran' adalah untuk memberi panduan pengawalan keselamatan fizikal serta selenggaraan perkakasan dan persekitaran bagi menyokong keperluan keselamatan ICT.

### 5.2. Prosedur Kawalan Fizikal Dan Persekitaran

#### 5.2.1. Keperluan Umum

a. Semua aset yang telah disenaraikan dalam Borang A atau borang aset sedia ada Kerajaan, terutama sekali aset persekitaran dan keselamatan fizikal hendaklah dikenalpasti kedudukan dan kesesuaiannya untuk menyokong operasi.

b. Tempat untuk simpanan rekod-rekod pematuhan keselamatan ICT hendaklah dikenalpasti dan lokasi tersebut hendaklah dikawal.

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

   i. Sistem kawalan fizikal hendaklah berfungsi dengan sempurna dan senarai pekerja hendaklah dikemaskini dari masa ke semasa,
   ii. Buku catitan berasingan hendaklah disediakan untuk merekodkan pergerakan keluar/masuk pelawat atau pihak selenggaraan perkakasan dalam bilik pelayan,
   iii. Penghawa dingin yang sesuai dengan kawalan kelembapannya mengikut spesifikasi perkakasan dalam Bilik Pelayan (*server room*),
   iv. Keupayaan UPS untuk membekalkan kuasa untuk masa yang diperlukan sebelum janakuasa tunggusedia (*standby generator*)

(jika ada) mula berfungsi atau sebelum sistem pelayan dimatikan (*shutdown*) dengan betul.

v. Kewujudan janakuasa tunggusedia untuk membekalkan kuasa jika perlu.

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

vii. Ruang khas yang selamat dan tahan kebakaran disediakan untuk menyimpan media backup.

viii. Selenggaraan berjadual yang perlu dilakukan mengikut panduan pembekal perkakasan. Semua rekod selenggaraan hendaklah disimpan dalam tempat selamat.

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

e. Kerja-kerja selenggaraan yang dijalankan oleh perkerja kontrak hendaklah disemak oleh kakitangan Jabatan yang bertanggungjawab. Semakan dibuat secara pensampelan (*sampling)* atau keseluruhan bergantung kepada perkara atau peralatan yang disemak.

## Seksyen 6. Pengurusan Operasi dan Rangkaian

### 6.1. Tujuan Umum

Tujuan Prosedur ini adalah untuk menentukan bahawa amalan operasi, kendalian, perubahan dan pembaikan sistem dilaksanakan dengan teratur dengan menggunakan borang-borang yang berkaitan.

### 6.2. Prosedur Pengurusan Operasi dan Rangkaian

#### 6.2.1. Pengurusan Konfigurasi

##### 6.2.1.1. Pengurusan Konfigurasi Perkakasan

a. Konfigurasi perkakasan, perisian dan rangkaian hendaklah dicatit atau dicetak dan disimpan sebagai *snapshot* untuk rujukan.

b. Sekiranya insiden atau masalah berlaku, *snapshot* konfigurasi ini hendaklah dibandingkan dengan konfigurasi sebenar.

c. Cetakan konfigurasi hendaklah disimpan ditempat selamat.

##### 6.2.1.2. Pengurusan Konfigurasi Teknikal

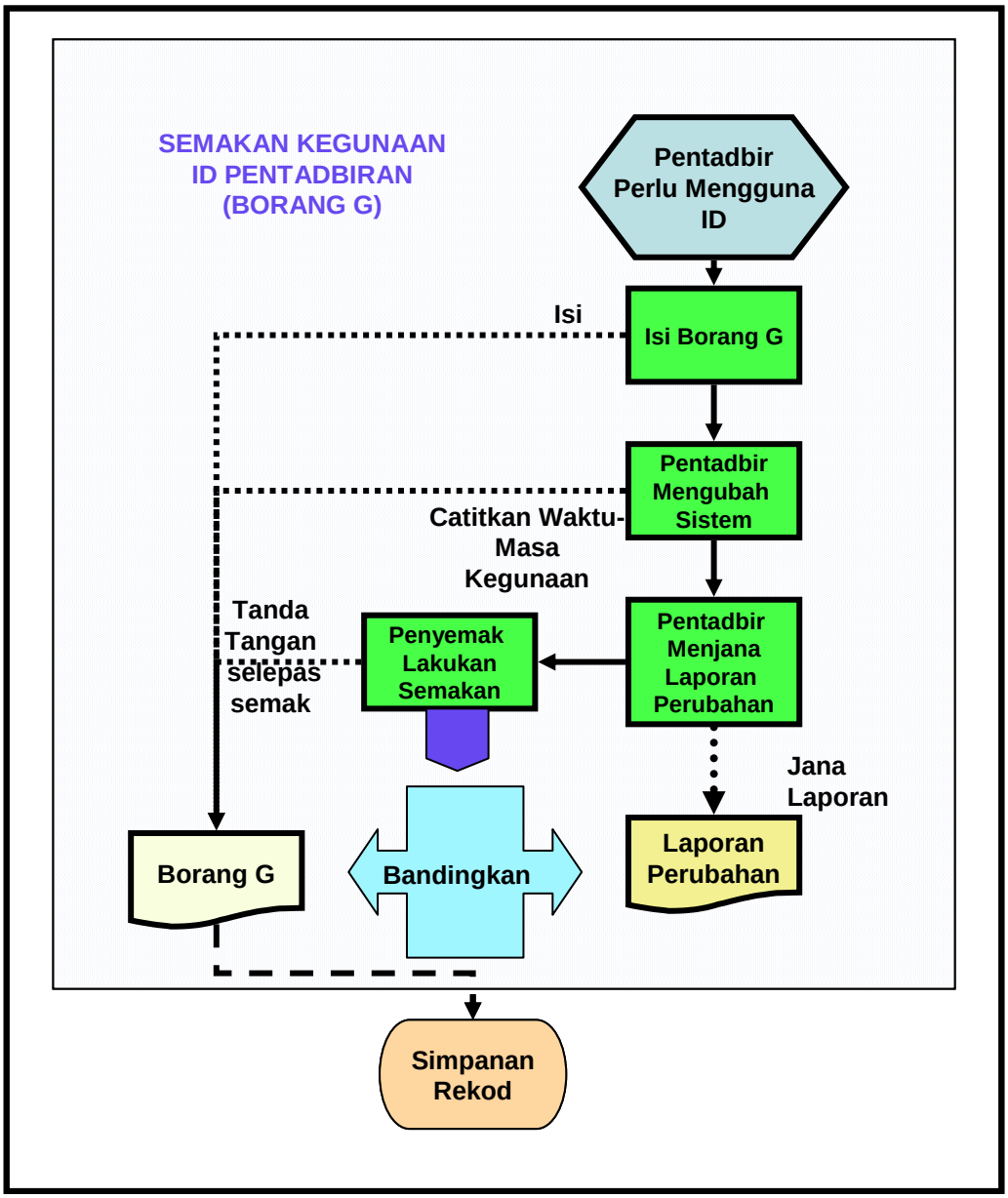
a. Konfigurasi teknikal adalah bertujuan memantapkan prestasi dan keselamatan sistem. Perubahan teknikal tidak melibatkan perkakasan melainkan konfigurasi berikut:

   i. Polisi firewall, Intrusion Detection Systems (IDS) atau Intrusion Protection Systems (IPS).

   ii. Alamat IP rangkaian dan pengasingan LAN (*LAN segments*).

b. Sekiranya perubahan konfigurasi perkakasan tersebut perlu dilakukan dengan menggunakan ID pentadbiran, maka

hendaklah direkodkan dengan menggunakan Borang G mengikut prosedur dalam Rajah 3:




Rajah 3 : Proses Kegunaan ID Pentadbir

c. Laporan perubahan yang dilakukan hendaklah dicetak dan dibandingkan tempoh kegunaannya yang dicatitkan dalam Borang G.

d. Rekod-rekod perubahan konfigurasi (sebelum dan selepas perubahan) hendaklah disimpan ditempat yang selamat.

### 6.2.1.3. Perubahan Konfigurasi Sementara

a. Perubahan sementara juga tertakluk kepada prosedur seperti **Rajah 3 : Proses Kegunaan ID Pentadbir.**

b. Permohonan peruba**han sementara boleh dibuat atas keperluan** penyelesaian insiden atau masalah yang dilaporkan melalui Borang D, dan borang tersebut hendaklah dirujuk dalam catitan.

c. Pemohon hendaklah memberi butir-butir perubahan konfigurasi sementara secara bertulis atau emel dan disalurkan kepada Penjaga Aset untuk pertimbangan dan kelulusan. Maklumat yang perlu dikemukakan untuk pertimbangan seperti berikut:

   i. Sebab-sebab keperluan perubahan sementara,

   ii. Tempoh perubahan sementara,

   iii. Risiko perubahan sementara itu, dan

   iv. Cara mengatasi atau mengawal risikonya.

d. Tentukan bahawa semua perubahan sementara dilaksanakan dalam tempoh yang diluluskan dan segala konfigurasi diubah semula ke konfigurasi asal melainkan konfigurasi baru diperlukan untuk menyelesaikan insiden atau masalah yang dilaporkan.

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

   i. Semua aktiviti kerja perubahan hendaklah dicatitkan oleh pelaksana perubahan, manakala log perubahan perlu

dijana untuk semakan Penjaga Aset selepas kerja-kerja perubahan dijalankan dan,

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

### 6.2.1.4. Perubahan Konfigurasi Dalam Keadaan Kecemasan

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

b. Perubahan kecemasan tertakluk kepada prosedur seperti dalam **Rajah 3 : Proses Kegunaan ID Pentadbir**, 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. 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 adalah perlu (dan tidak ada jalan lain atau tidak boleh ditangguhkan) dan meluluskannya sebelum perubahan dijalankan oleh Penjaga Aset.**

f. **Untuk aplikasi atau sistem dalam Kategori 1, semua perubahan konfigurasi hendaklah direkodkan selepas**

**perlaksanaan (*retrospectively*) dan semua jejak Audit hendaklah disimpan untuk semakan. Jejak Audit ini hendaklah dilampirkan kepada Borang G.**

a. Pemilik Aset hendaklah:

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.

### 6.2.2. Pengasingan Kerja

a. **Pengasingan kerja hendaklah dilaksanakan untuk aplikasi atau sistem dalam Kategori 1.**

b. Logon ID hendaklah diwujudkan secara berasingan untuk tugasan yang memerlukan pengasingan kerja, (walaupun digunakan oleh seorang individu sahaja). Ini adalah untuk memudahkan pemantauan kegunaan ID, sesuai dengan kerja-kerja yang dijalankan.

c. Semua aktiviti penting dalam kegunaan ID berkenaan hendaklah mempunyai Jejak Audit dan **ini diwajibkan untuk aplikasi atau sistem dalam Kategori 1**.

### 6.2.3. Kawalan Kegunaan ID Yang Tinggi Hak Capaiannya

a. ID Pentadbir Sistem (*Administration ID*), '*Root*' atau '*Superuser*' hendaklah wujud untuk setiap komponen sistem, sama ada pelayan, OS, pangkalan data, alat rangkaian, firewall, dan aplikasi. Kegunaan ID seumpama ini yang hak capaiannya (*access privileges*) paling tinggi, perlu dikawal kegunaanya.

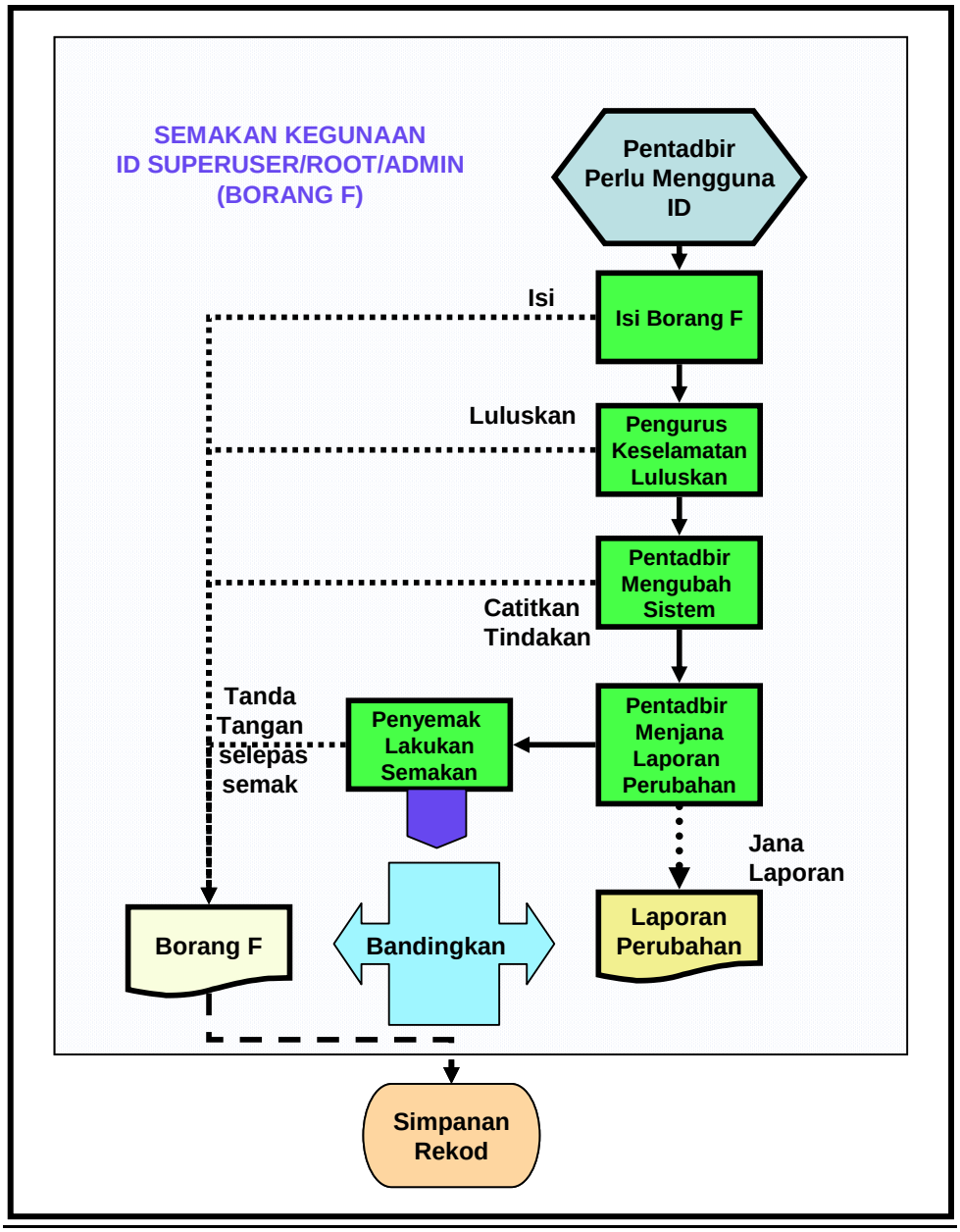
b. **Untuk aplikasi atau sistem dalam Kategori 1**, ID khusus dan terhad hendaklah diwujudkan bagi tujuan yang ditetapkan seperti melakukan *backup*, mengaktifkan perkhidmatan yang diperlukan (*services*), mengubah konfigurasi dan memantau kegunaan sistem (*system resource monitoring and network utilisation monitoring*).

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

d. Sekiranya ID yang tinggi hak capaiannya perlu digunakan, maka pastikan bahawa semua permohonan dan gerak langkah penggunaan dipantau menerusi proses dalam Rajah 4.

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

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




Rajah 4 : Proses Kegunaan ID Superuser/Root/Admin

### 6.2.4. Prosedur Kendalian (Operating Procedures) dan Dokumentasi

a. Semua prosedur operasi hendaklah didokumenkan dan pastikan dokumentasi tersebut mempunyai kawalan perubahan dokumentasi.

b. Dokumentasi berkaitan perlu disebarkan kepada semua yang berkenaan dengan arahan untuk melupuskan muka surat dokumentasi yang lama yang telah diganti atau dibatalkan.

c. Senarai penerima dokumentasi disediakan supaya pembahagian dokumentasi tepat dan terkawal.

### 6.2.5. Selenggaraan Aplikasi atau Sistem

a. Langkah terperinci untuk selenggaraan setiap komponen sistem hendaklah didokumenkan mengikut kawalan dokumen.

b. Satu jadual selenggaraan sistem perlu disediakan untuk semua perkakasan dengan butiran yang perlu diselenggarakan pada tahap jadual tertentu. Satu jadual perlu disediakan oleh penyelenggara (pihak ketiga) untuk kelulusan bahagian ICT Jabatan.

c. Sekiranya jadual selenggara perlu ditangguhkan, maka aktiviti tersebut hendaklah dilakukan secepat mungkin selepas penangguhan.

d. Perkakasan yang diganti atau dibaiki hendaklah dicatitkan dan rekod konfigurasi hendaklah dikemaskini sekiranya berlaku perubahan perkakasan atau komponen.

e. Untuk selenggaraan yang dilakukan oleh pihak ketiga, pastikan penggunaan ID aplikasi atau sistem yang terhad untuk kegunaan mereka.

### 6.2.6. Perjanjian Tahap Perkhidmatan (SLA)

a. Tentukan bahawa peruntukan SLA memenuhi keperluan keselamatan sistem.

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

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

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

### 6.2.7. *Backup* dan *Media Backup*

a. Uji media *backup* dari masa ke semasa untuk memastikan ia berfungsi dengan baik.

b. Simpan rekod untuk menjejak kegunaan dan kitaran gunaan setiap media cetak.

c. Adakan jadual *backup* yang bersesuaian dengan kegunaan aplikasi.

d. **Untuk Kategori 1, *backup* penuh data (*full data backup*) hendaklah dilakukan setiap minggu manakala *backup* data tambahan (*incremental backup*) hendaklah dilakukan setiap hari.**

e. Pastikan bahawa fail penting tidak disimpan dalam PC atau notebook. Ruang bagi pengguna hendaklah disediakan dalam pelayan supaya *backup* berjadual boleh dilakukan.

f. Pengguna hendaklah melakukan *backup* sendiri bagi fail-fail penting dan menyimpannya di tempat yang selamat.

### 6.2.8. Komputer Kerajaan Negeri

a. Pihak ICT Jabatan bertanggungjawab menguruskan pemasangan komputer di premis Jabatan termasuk sambungan ke rangkaian Melaka*Net.

b. Pengguna tidak dibenarkan mengubah pemasangan komputer atau menyambung komputer ke rangkaian lain (contoh:

menerusi dial-up ‘wireless LAN’, 3G kecuali Bluetooth) tanpa kebenaran pihak ICT Jabatan.

c. Pengguna dikehendaki bekerjasama membuat ujian atau mengubah sementara sambungan ke rangkaian atas arahan kakitangan selenggaraan BTMK atau ICT Jabatan semasa penyiasatan penyelesaian masalah secara jarak jauh (*remote*).

### 6.2.9. Rangkaian Tanpa Wayar

a. Rangkaian tanpa wayar (Open Wireless) yang disediakan di Jabatan Kerajaan Negeri Melaka adalah hanya untuk kegunaan orang awam dan pelawat yang datang berurusan.

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

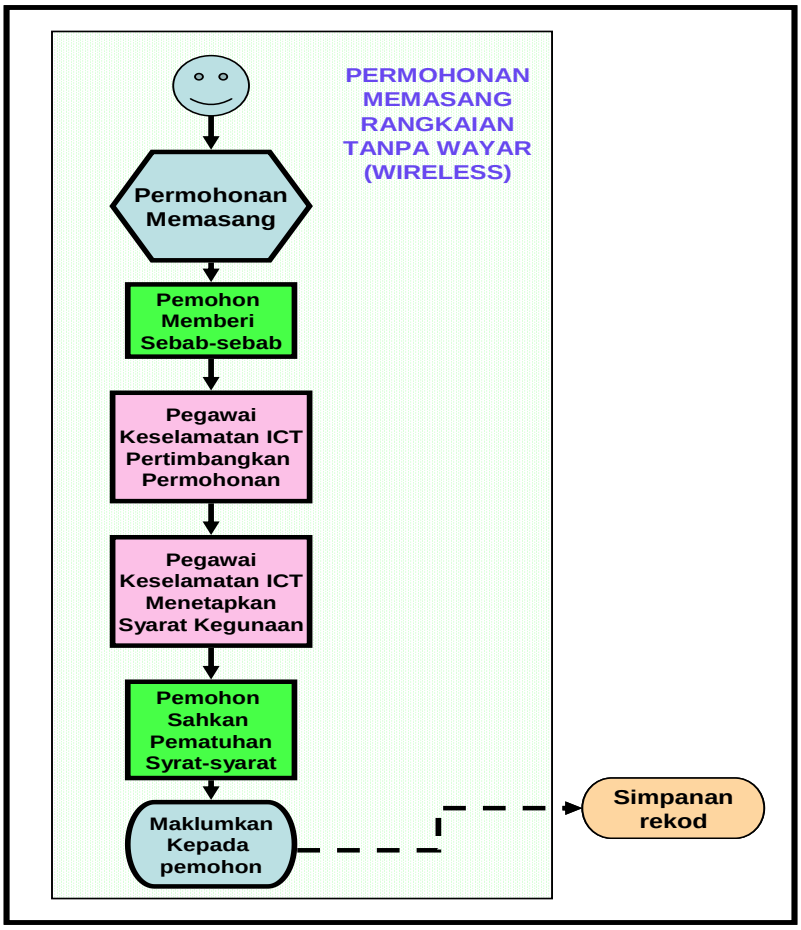
c. Pengguna seperti bil. 6.2.9 (a) hendaklah memohon kelulusan dari Pegawai Keselamatan ICT Kerajaan Negeri, melalui Ketua Jabatan/Pegawai pengawal, dengan bersurat atau emel dan hendaklah menyatakan justifikasi keperluan.

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

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

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

g. Aliran proses permohonan ditunjukkan dalam Rajah 5:




Rajah 5 : Proses Permohonan Rangkaian Tanpa Wayar

### 6.2.10. Perancangan Kapasiti Perkakasan

a. Bahagian ICT Jabatan hendaklah memantau semua sumber secara berkala atau sekurang-kurangnya sekali setahun bagi menentukan keupayaan perkakasan sedia ada

Diantara perkakasan yang perlu dipantau adalah seperti berikut:

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

- Pastikan berfungsi dengan sempurna.

ii) Aplikasi dan Sistem:

- Masa respon mengikut piawaian yang telah ditetapkan.

iii) Cakera keras:

- Kapasiti setoran yang mencukupi.

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

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

d. Bajet dan jangka masa hendaklah diambilkira semasa membuat perancangan naiktaraf atau gantian sistem.

e. Kos naiktaraf hendaklah dibandingkan dengan kos gantian serta tempoh sokongan (support) perkakasan oleh pembekal sebelum sesuatu keputusan dibuat.

### 6.2.11. Penggunaan Perisian Anti-Virus dan Anti-Malware

a. BTMK bersama pihak ICT Jabatan-Jabatan hendaklah menetapkan perisian *anti-virus* dan *anti-malware* untuk diseleraskan dalam Kerajaan Negeri atau Jabatan.

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

c. Pengguna tidak dibenarkan mengubah konfigurasi komputer, khususnya berkaitan pengemaskinian perisian *anti-virus* dan *anti-malware* secara automatik.

### 6.2.12. Simpanan Rekod dan Pengurusan Kualiti

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

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

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

### 6.2.13. Pemantauan Aktiviti Pelbagai

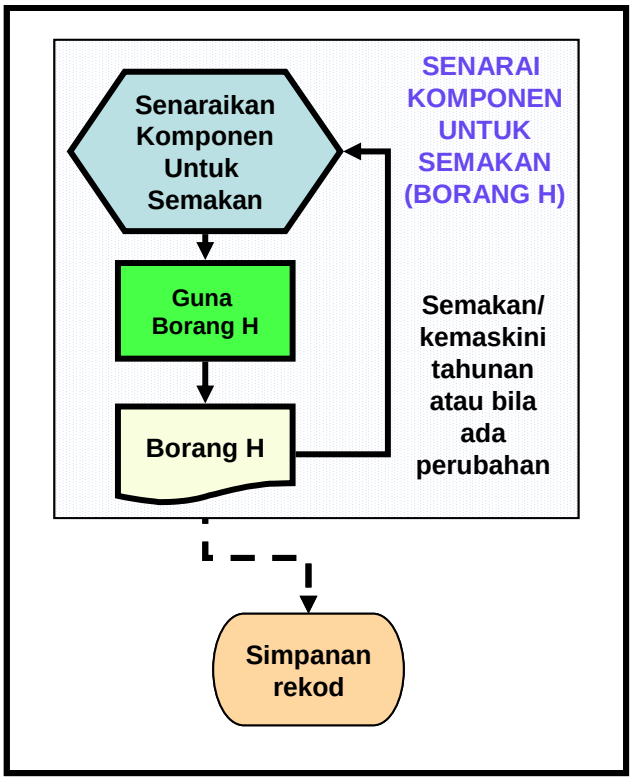
a. Selain daripada pemantauan kegunaan ID *Superuser*/ *Root*/*Admin* dan ID Pentadbiran (Sistem, Pangkalan Data, Keselamatan) beberapa aktiviti lain perlu juga dipantau. Pemantauan tersebut bergantung kepada tahap kritikal aplikasi dan sebagainya. Di antara aktiviti atau perkara yang perlu dipantau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

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

b. Senarai aktiviti, komponen atau perkara yang dianggap perlu dipantau hendaklah dicatitkan dalam Borang H. Proses tersebut seperti Rajah 6.

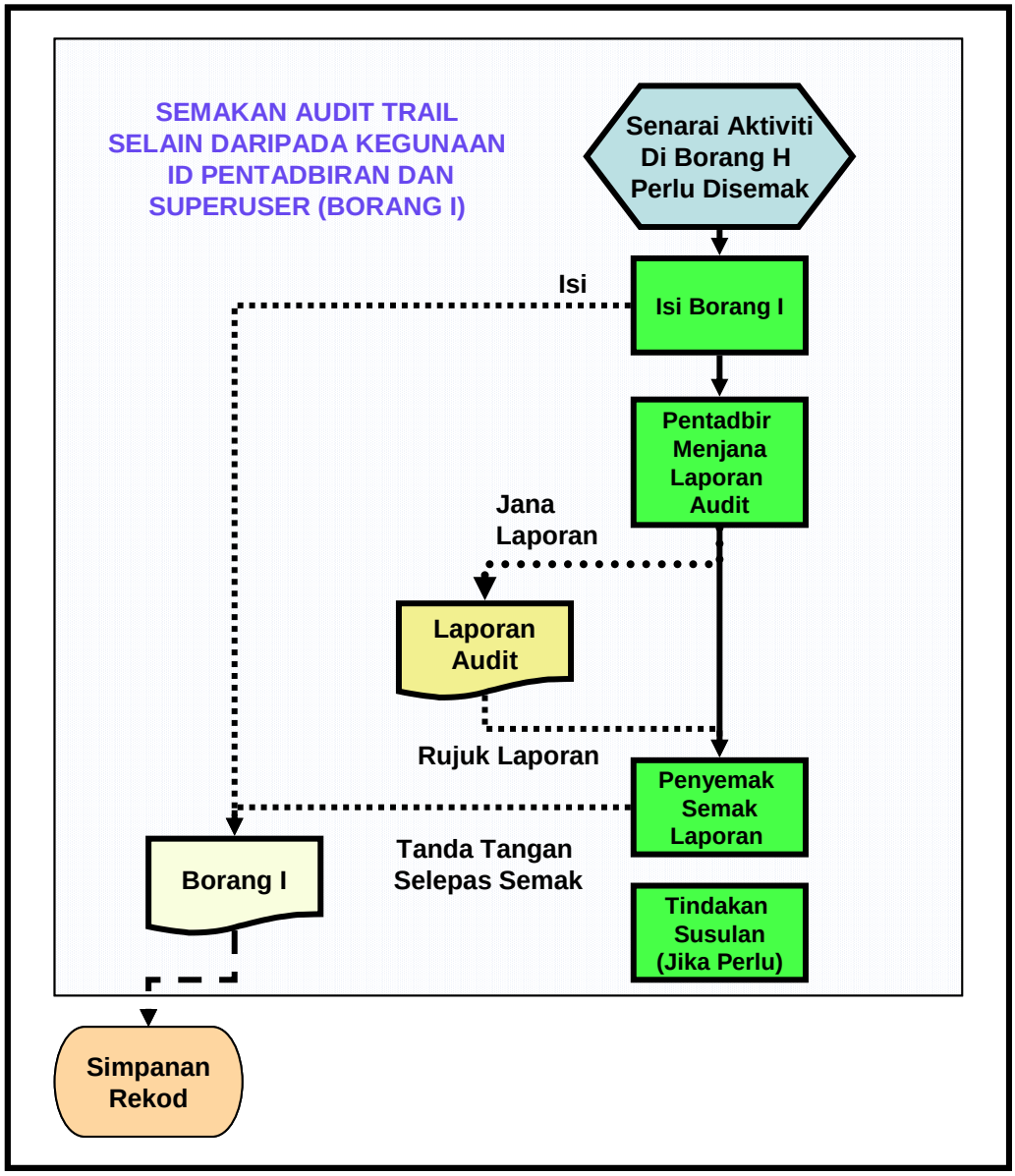
c. Senarai tersebut hendaklah diluluskan oleh Pegawai Keselamatan ICT.

d. Proses semakan komponen-komponen senarai tersebut boleh dilakukan menggunakan Borang I mengikut proses seperti Rajah 7.




Rajah 6 : 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.




Rajah 7 : Proses Semakan Komponen

## Seksyen 7. Kawalan Capaian Logikal

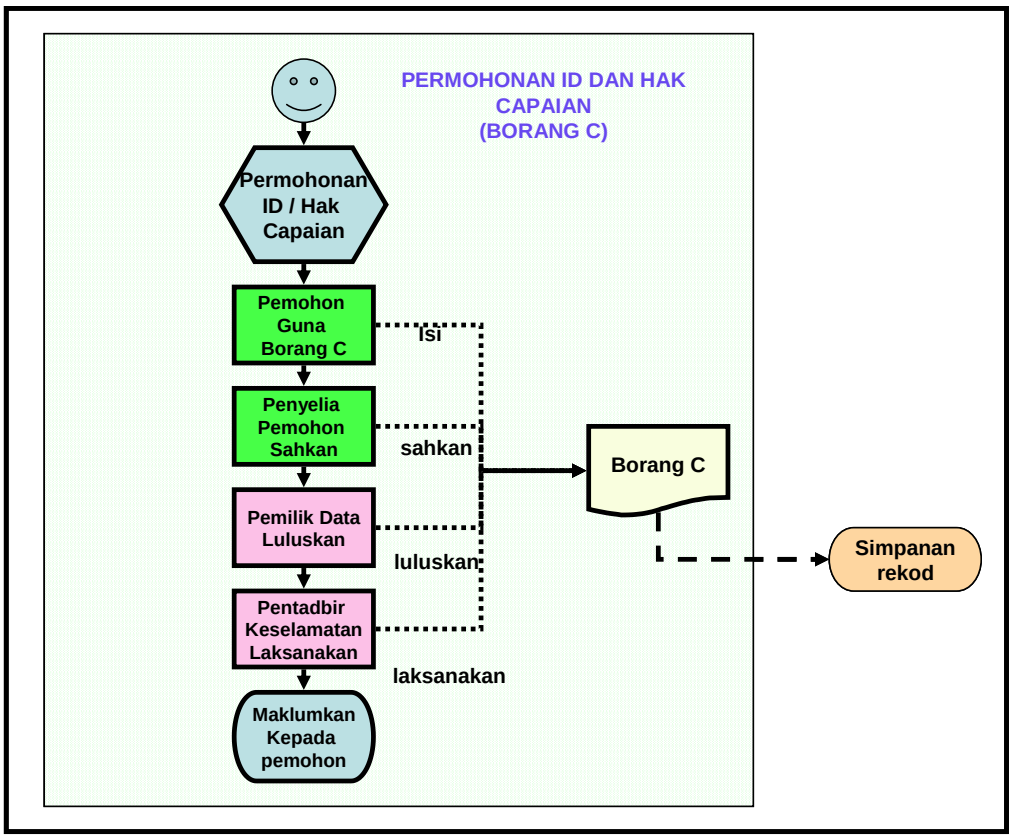
### 7.1. Tujuan Umum

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

### 7.2. Prosedur Kawalan Capaian Logikal

#### 7.2.1. Kawalan Capaian Logikal Secara Umum

a. Setiap pengguna hendaklah memohon ID serta hak capaian dengan menggunakan Borang C mengikut proses dalam Rajah 8 kecuali kemudahan permohonan ID yang disediakan secara *online*.




Rajah 8 : Proses Permohonan ID/Hak Capaian dan/atau Perubahan Aplikasi/Sistem

### 7.2.2. Perlindungan Kata Laluan

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

### 7.2.3. Pentadbiran ID dan Capaian Logikal

a. Setiap Ketua Jabatan hendaklah menyediakan senarai terkini pengguna aplikasi atau sistem dalam tadbirannya sekurang-kurangnya sekali setahun. Pentadbir Keselamatan hendaklah menyemak senarai tersebut dan bandingkan dengan borang permohonan dan pelupusan ID sekurang kurangnya sekali setahun untuk penyelarasan. Proses yang boleh diikuti adalah dalam **Rajah 7 : Proses Semakan Komponen.**

### 7.2.4. Pemansuhan Hak Capaian Logikal

a. Hak capaian sesuatu pengguna yang tidak diperlukan lagi hendaklah dimansuhkan.

b. ID pengguna yang tidak aktif selama enam puluh (60) hari berturut-turut hendaklah dimansuhkan, kecuali ID yang memang dikenalpasti digunakan hanya pada masa tertentu.

c. Penggantungan ID hendaklah diku**a**tkuasakan secara automatik apabila berlaku tiga kesalahan kata laluan berturut-turut. Pengguna hendaklah memohon untuk mengguna ID itu kembali (*reactivated*). Ini diwajibkan untuk sistem yang ditauliahkan selepas akhir tahun 2008.

### 7.2.5. Pemantauan Kegunaan Hak Capaian

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

masa ke semasa mengikut proses dalam Rajah **8** : Proses Permohonan ID/Hak Capaian, **Rajah 4 : Proses Kegunaan ID Superuser/Root/Admin** dan **Rajah 6 : Proses Merekod Senarai Komponen Untuk Semakan**.

b. Proses seperti perkara 7.2.5 (a) adalah untuk memastikan sistem digunakan dengan betul dan teratur dan tidak ada unsur-unsur yang mencurigakan. Diantara perkara yang perlu diperhatikan ialah:

   i. Kegagalan memasuki sistem atau cubaan memasuki bahagian-bahagian sistem atau aplikasi yang diluar hak capaian pengguna berkenaan,
   ii. Kegunaan ID kritikal yang hak capaiannya luas,
   iii. Corak kegunaan sistem yang luar biasa (misalnya luar dari waktu pejabat biasa).

## Seksyen 8. Pembangunan dan Penyelenggaraan Aplikasi

### 8.1. Tujuan Umum

Tujuan prosedur ini adalah untuk memastikan bahawa pembangunan aplikasi dan penyelenggaraan aplikasi dijalankan dengan betul untuk menjamin keselamatan aplikasi.

### 8.2. Prosedur Pembangunan dan Penyelenggaraan Aplikasi

#### 8.2.1. Spesifikasi Keselamatan Dalam Aplikasi

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

b. Rekaan sistem hendaklah mempunyai ciri mengawal ketepatan dan integriti data. Ini dicapai dengan penapisan data (*validation*) semasa peringkat kemasukan atau perubahan data. Tapisan tersebut hendaklah merangkumi format data (contoh: tarikh atau angka hendaklah dikuatkuasakan supaya dimasukkan dengan betul), jarak data yang ditetapkan (*valid data range*) dan data yang wajib dimasukkan (*compulsory data*).

c. Aplikasi hendaklah direkabentuk mengikut pematuhan garis panduan keselamatan yang boleh didapati dari dokumen, badan dan sumber yang boleh dipercayai seperti:

   i. Dokumen ISO 27002 – Code of Practice for Information Security,
   ii. Dokumen ‘A Guide to Building Secure Web Applications and Web Services’ dari OWASP – www. Owasp.org.

d. Pihak Ketiga yang membangunkan aplikasi hendaklah mengulas secara bertulis rekabentuk aplikasi tersebut dengan ciri-ciri keselamatan seperti berikut:

   i. Peniliaian 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,
   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,
   iv. 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.

### 8.2.2. Pembangunan dan Penyelenggaraan Aplikasi

a. Aplikasi boleh diterima selepas ujian dan pengesahan kawalan proses pembangunan dan penyerahan aplikasi berikut dilaksanakan:

   i. Keperluan dan perlaksanaan aplikasi didokumenkan,
   ii. Perubahan aplikasi dikawal dengan baik,
   iii. Paparan amaran dan makluman yang sesuai dengan keadaan dipamerkan bila perlu (*context sensitive warning, error or help messages*),
   iv. Penyemakan integriti (*integrity checks*) di laksanakan di bahagian-bahagian perisian yang berpatutan,

v. Proses ujian aplikasi dilakukan dengan sempurna dan menyeluruh,
vi. Latihan pengguna dilaksanakan,
vii. Dokumentasi pemasangan, kegunaan, pembetulan dan senggaraan aplikasi disediakan.

## Seksyen 9. Pengurusan Insiden

### 9.1. Tujuan Umum

Prosedur ini adalah untuk menghuraikan langkah-langkah untuk melaporkan insiden atau masalah dan urutan tindakan penyelesaian masalah.

### 9.2. Prosedur Pengurusan Insiden

#### 9.2.1. Laporan Insiden dan Penyelesaian

a. Setiap insiden hendaklah dilaporkan menggunakan sistem Intranet yang sedia ada. Jabatan yang tidak menggunakan Intranet boleh mengguna Borang D. Rajah 9 adalah untuk proses menyelesaikan insiden atau masalah yang merujuk kepada penggunaan Borang D:

b. Laporan insiden boleh diterima secara lisan atau emel tetapi perlu disusuli dengan Borang D atau paparan dalam sistem Intranet untuk laporan insiden yang lengkap.

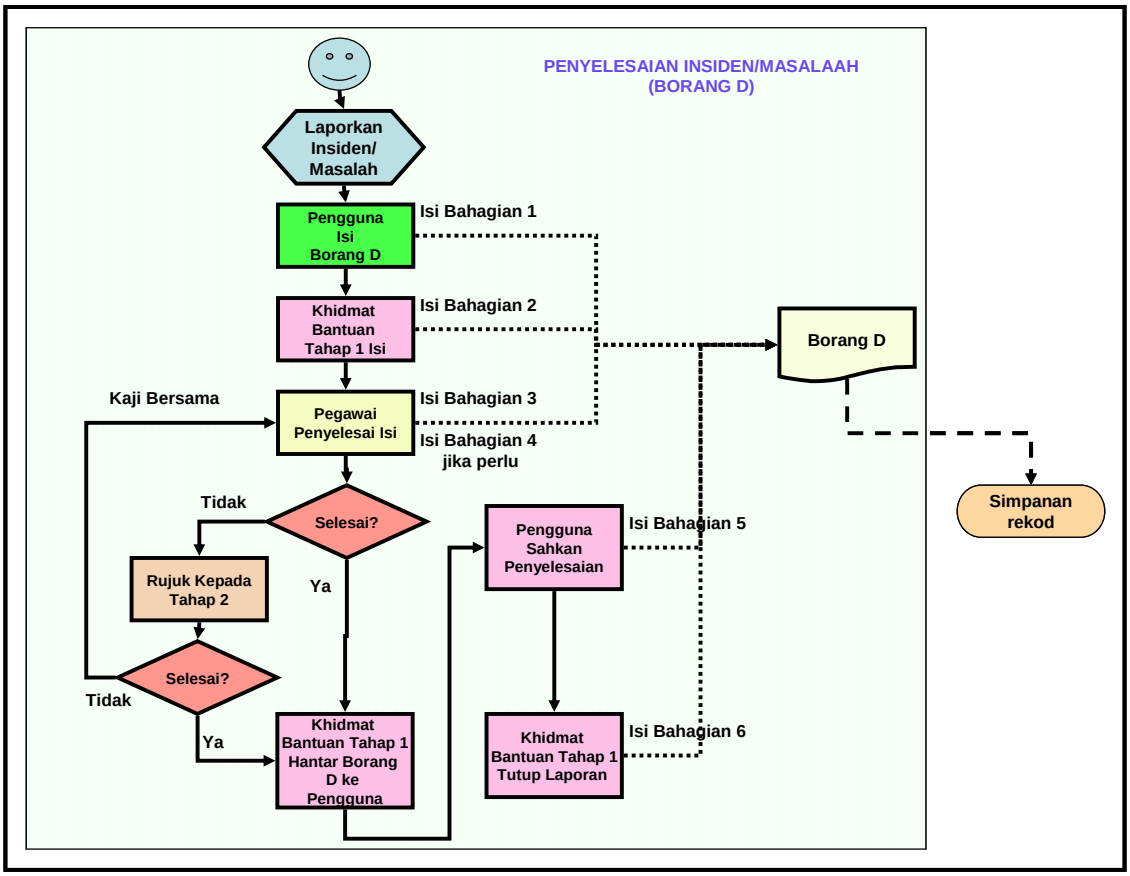
c. Peruntukkan setiap inisden kepada kakitangan bantuan bertugas untuk penyelesaian mengikut prioriti.

d. Kakitangan bantuan yang ditugaskan hendaklah merangka tindakan pembetulan yang sesuai untuk menyelesaikan masalah atau insiden.

e. Semua yang terlibat untuk menyelesaikan sesuatu insiden perlu bekerjasama dan berhubung rapat untuk menyelesaikan insiden tersebut.

f. Sekiranya penyelesaian insiden adalah luar dari bidang tugas atau bidang pengalaman kakitangan bantuan, maka laporan insiden itu perlu dimajukan ke Khidmat Bantuan Tahap 2.

g. Bagi insiden keselamatan yang melibatkan serangan siber, SOP Pengurusan Pengendalian Insiden Keselamatan ICT perlu dipatuhi.



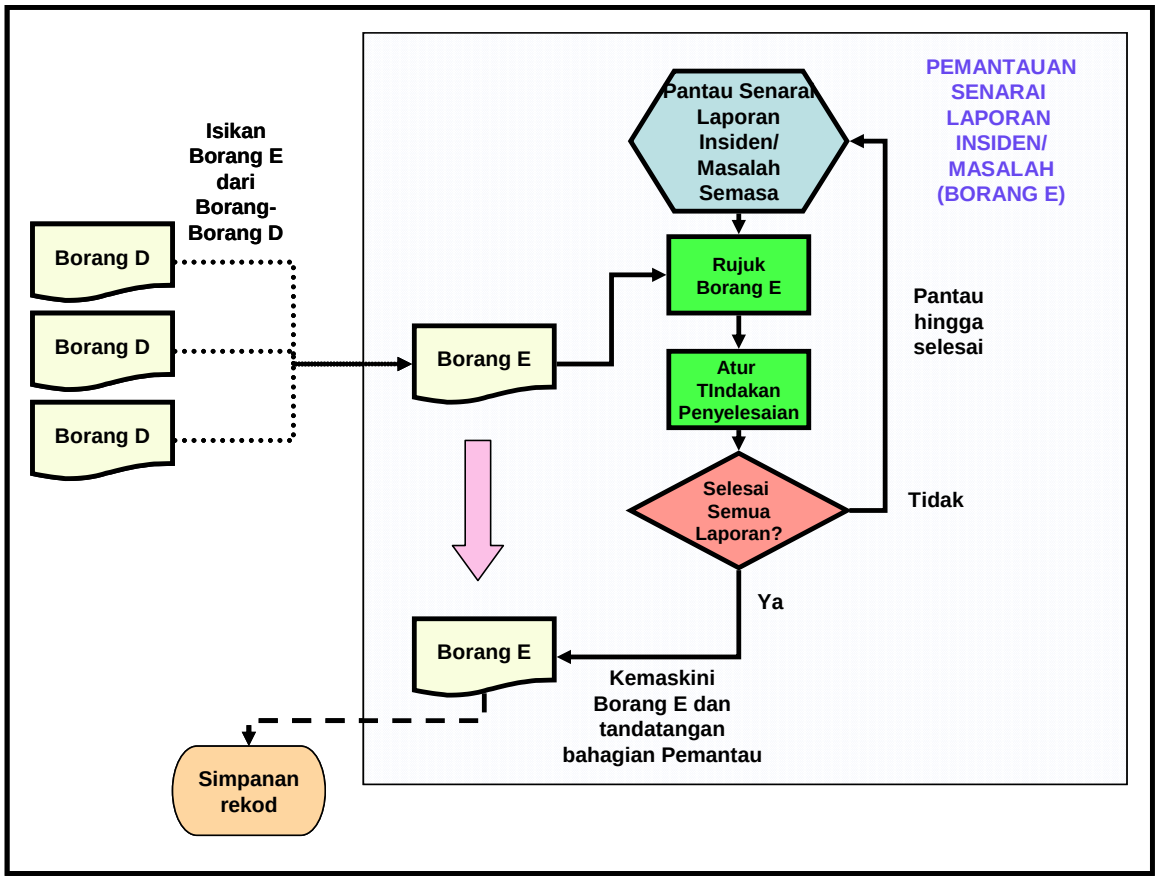

Rajah 9 : Proses Laporan Insiden dan Penyelesaian Insiden

### 9.2.2. Pemantauan Penyelesaian Laporan Insiden

a. Pemantauan penyelesaian laporan insiden hendaklah menggunakan Borang E dan mengikut proses dalam Rajah 10 kecuali insiden keselamatan yang melibatkan serangan siber hendaklah mematuhi SOP Pengurusan Pengendalian Insiden Keselamatan ICT.

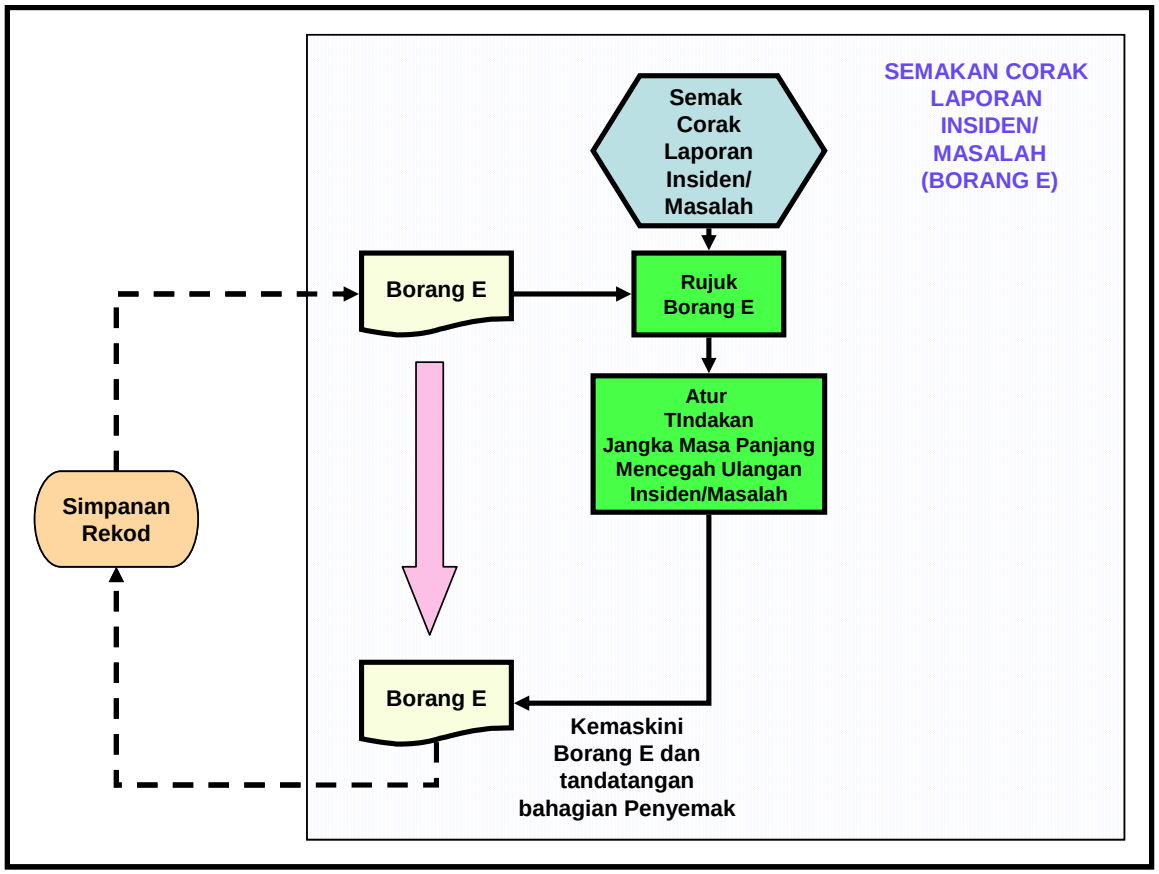
b. Semua maklumat ringkas dalam Borang D atau sistem Intranet hendaklah dimasukkan dalam Borang E untuk pemantauan oleh pihak Pengurusan ICT.

c. Tindakan penyelesaian hendaklah diaturkan dan apabila semua laporan dalam senarai sesuatu Borang E telah selesai, maka Borang E berkenaan hendaklah disimpan dalam simpanan rekod.




Rajah 10 : Proses Pemantauan Penyelesaian Insiden

d. Kajian hendaklah dibuat dari semasa ke semasa untuk mengenalpasti corak atau *trend* laporan insiden dan merangka penyelesaian jangka masa panjang supaya insiden yang kerap berlaku dapat dikawal atau dikurangkan. Untuk tujuan ini, Borang E boleh digunakan mengikut proses dalam Rajah 11.




Rajah 11 : Proses Semakan Laporan Insiden

## Seksyen 10. Pengurusan Kesinambungan Perkhidmatan

### 10.1. Tujuan Umum

Tujuan prosedur ini adalah untuk memastikan bahawa 'Pengurusan Kesinambungan Perkhidmatan' diurus dan dirangka dengan tepat dan dengan perbelanjaan yang berpatutan.

### 10.2. Prosedur Pengurusan Kesinambungan Perkhidmatan

#### 10.2.1. Kewajipan Merangka Kesinambungan Perkhidmatan

a. Jawatankuasa untuk mengkaji dan merancang Pelan Kesinambungan Perkhidmatan (BCP) hendaklah dibentuk.

b. Kakitangan-kakitangan yang terlibat hendaklah terdiri dari mereka yang berpengalaman dan memahmi konteks perkhidmatan dan keperluan kesinambungan perkhidmatan.

c. Kemajuan rancangan hendaklah dipantau.

#### 10.2.2. Analisa Dan Mengenalpasti Perkhidmatan Penting

a. Proses atau metodologi yang diiktiraf hendaklah digunakan.

a. Perkhidmatan yang penting hendaklah dikenalpasti dan rancangan baikpulih perkhidmatannya hendaklah diperincikan apabila berlaku gangguan.

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

### 10.2.3. Perlaksanaan Pelan dan Ujian

a. Pelan kesinambungan perkhidmatan hendaklah dirangka dan diuji kesesuaian dan ketepatannya dari masa ke semasa.

b. Ujian pemulihan ICT hendaklah dilakukan lebih kerap dari ujian keseluruhan.

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

## Seksyen 11. Pematuhan

### 11.1. Tujuan Prosedur

Tujuan prosedur ini adalah untuk 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 perlaksanaan keselamatan dan mengurangkan gangguan sistem.

### 11.2. Prosedur Pematuhan

#### 11.2.1. Pematuhan Kepada Keperluan Undang Undang

a. Khidmat nasihat berkaitan undang undang dan garsipanduan yang berkaitan dengan operasi Jabatan hendaklah dikaji dan diambil jika perlu.

b. Langkah untuk mematuhi keperluan undang-undang, peraturan-peraturan serta arahan atau garis panduan Kerajaan hendaklah diaturkan.

#### 11.2.2. Semakan Polisi Keselamatan Dan Pematuhan

a. Polisi Keselamatan hendaklah disemak dari masa ke semasa untuk menentukan ia menepati keperluan semasa dan masa akan datang.

b. Pengarah-Pengarah Jabatan hendaklah merangka rancangan untuk mengguna ukuran atau KPI untuk mengukur tahap pematuhan Polisi Keselamatan Jabatan.

### 11.2.3. Keperluan Audit

a. 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.

### 11.2.4. Audit Dalaman dan Luaran

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

i. menjalankan audit pemantauan dalam Jabatan dari masa ke semasa,

ii. tidak perlu terdiri daripada kalangan teknikal ICT tetapi hendaklahlah orang terlatih yang boleh memahami keperluan polisi atau standard atau prosedur, dan memastikan tahap pematuhan polisi atau standard atau prosedur, serta merekodkan hasil kajiannya untuk perhatian dan tindakan pengurusan Jabatan.

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

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.

c. Perunding yang berkemampuan hendaklah digunakan untuk menjalankan Audit Luaran terhadap polisi, standard dan prosedur keselamatan ICT.

### 11.2.5. Hak Capaian Untuk Juru Audit

a. Pastikan bahawa juru audit diberikan hak capaian terhad dan terkawal jika perlu dalam tempoh audit. Batalkan hak capaian selepas audit selesai.

## DEFINISI POLISI, STANDARD, GARIS PANDUAN DAN PROSEDUR

### 1. Polisi

Polisi adalah kenyataan atau arahan ringkas yang menggambarkan tujuan atau sasaran yang hendak dicapai. Ia biasanya ringkas supaya senang difahami dan diingati untuk dipatuhi oleh semua yang terlibat.

Polisi adalah tahap kenyataan yang paling tinggi (*higher-level requirement statements*) berbanding dengan standard, walaupun kedua duanya hendaklah dipatuhi.

### 2. Standard

Standard memberi arahan atau keperluan yang lebih khusus dan lebih jelas (*detailed*) supaya ciri-ciri perlaksanaannya dapat difahami dan dipatuhi. Standard boleh dibentuk khusus untuk sesuatu situasi atau keperluan, sesuai dengan suasana operasi yang disasarkan.

Polisi kebiasaannya jarang-jarang bertukar tetapi standard boleh bertukar mengikut perkembangan masa, teknologi, perubahan sistem, suasana atau lokasi kerja, ancaman dan risiko.

### 3. Garis Panduan

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

### 4. Prosedur

Prosedur kadangkala dipanggil ‘operating procedures’, ‘standard operating procedures’ atau SOP. Prosedur adalah langkah-langkah yang khusus dan

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

Dalam siri dokumen-dokumen ini hanya prosedur-prosedur ‘common’ sahaja disediakan.

Contoh berikut berkaitan akses logikal memberi gambaran perbezaan antara polisi, standard, garis panduan dan prosedur.

- Polisi menerangkan keperluan untuk menguruskan akses logikal.
- Standard menerangkan aktiviti minima yang hendaklah dilakukan untuk menguruskan akses logikal. (Bergantung kepada domain polisi, standard mungkin tidak perlu diwujudkan.)
- Garis Panduan mencadangkan ciri ciri atau cara terbaik untuk menguruskan akses logikal.
- Prosedur menerangkan cara terperinci untuk menguruskan akses logikal, termasuk penimpanan rekod dan pemantauan.

## KEMBARAN : BORANG BORANG BERKAITAN PENTADBIRAN KESELAMATAN

**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: _____<br>Telefon: _____<br>Faks: _____<br>Emel: _____<br>T.Tangan :_____ | Nama: _____<br>Telefon: _____<br>Faks: _____<br>Emel: _____<br>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 Sistem / Operasi ICT**

| No Siri | |
|---|---|

| **TINDAKAN PENGGUNA** | |
|---|---|
| NAMA : | NO.TELEFON : |
| JAB/BAH/UNIT : | EMEL : |
| NAMA SISTEM/APLIKASI : | |
| PERUBAHAN/PERMOHONAN YANG DIPERLUKAN: | TANDATANGAN :<br><br>TARIKH : |
| **KELULUSAN PEMILIK APLIKASI / SISTEM / DATA** | |
| JENIS :<br>[ ] Permohonan baru [ ] Kemaskini Capaian<br>[ ] Penambahbaikan [ ] Pembatalan Capaian<br>[ ] Pertambahan modul / *page* baru | KEUTAMAAN :<br>[ ] MINOR<br>[ ] MAJOR<br>[ ] KRITIKAL |
| MAKLUMBALAS : | COP & TANDATANGAN :<br><br>TARIKH : |
| **TINDAKAN PEMBEKAL / PEMILIK APLIKASI / SISTEM / DATA** | |
| DESKRIPSI PERUBAHAN YANG DILAKUKAN : | STATUS :<br>[ ] SELESAI<br>[ ] TANGGUH |
| | VERSI LAMA (*jika ada*) :<br>_____<br>VERSI BARU (*jika ada*) :<br>_____ |
| | TARIKH SIAP : |
| **PENGESAHAN KETUA BAHAGIAN / UNIT** | |
| MAKLUMBALAS : | COP & TANDATANGAN :<br><br>TARIKH : |
| **PENGESAHAN PENGGUNA** | |
| MAKLUMBALAS/ CATATAN: | TANDATANGAN :<br><br>TARIKH : |

## 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 & WAKTU INSIDEN | | |
| 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, PC, switch, kebel dan sebagainya) | |
| | Pengenalan Perkakasan Sekiranya Ada (Aset) | |
| PENERANGAN INSIDEN/MASALAH TERPERINCI<br>(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 tiap tiap tindakan sekiranya memakan masa beberapa hari) | 1.<br>2.<br>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 | Tarkikh dan Waktu | 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. **Walaubagaimanapun untuk Aplikasi/Sistem dalam Kategori 1, semua aktiviti perlu direkodkan.**

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 | Fungsi Yang Ditugaskan Menjana Laporan Audit Trail (Jika berkenaan) | Fungsi Yang Ditugaskan 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. | | | | | | |

Tandatangan Pengesah Semakan : _____

Nama : _____ Fungsi : _____

Tarikh : _____

**BAHAGIAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI**
**JABATAN KETUA MENTERI MELAKA**