Lampiran kepada Surat Pekeliling Am Bilangan 2 Tahun 2021

versi 2.0

Garis Panduan

Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam

ISI KANDUNGAN

KAWALAN VERSI DOKUMEN v
AKRONIM DAN DEFINISI viii
1. PENGENALAN 1
2. TUJUAN 1
3. PELAKSANAAN PENGKOMPUTERAN AWAN DI DALAM PERKHIDMATAN AWAM 2
4. KLASIFIKASI MAKLUMAT ATAU DATA 3
4.1.1. Rasmi 3
4.1.2. Data Terbuka (*Open Data*) 4
4.1.3. Data Terkawal / Sensitif 4
4.1.4. Rahsia Rasmi 4
5. CIRI–CIRI ASAS DAN MODEL PERKHIDMATAN PENGKOMPUTERAN AWAN 5
5.1. Ciri-Ciri Asas Pengkomputeran Awan 5
5.1.1. Permintaan Secara Layan Diri (On Demand Self-Service) 5
5.1.2. Akses Rangkaian Yang Meluas (Broad Network Access) 5
5.1.3. *Resource Pooling* 5
5.1.4. Keanjalan Pantas (Rapid Elasticity) 5
5.1.5. Measured *Service* 5
5.2. Model Perkhidmatan Pengkomputeran Awan 6
5.2.1. Perisian Sebagai Perkhidmatan (Software-as-a-Service -SaaS) 6
5.2.2. Platform Sebagai Perkhidmatan (Platform-as-a-Services - PaaS) 6
5.2.3. Infrastruktur Sebagai Perkhidmatan (Infrastructure-as-a-Services - IaaS) 7
6. PENENTUAN MODEL PELAKSANAAN PENGKOMPUTERAN AWAN BAGI PERKHIDMATAN AWAM 8
6.2.1. *Private Cloud* 8
6.2.2. *Public Cloud* 10
6.2.3. *Hybrid Cloud* 10
7. RISIKO KESELAMATAN YANG PERLU DIPERTIMBANGKAN 11
7.2.1. Kedaulatan Data (Data Sovereignty) 11
7.2.2. Risiko Daripada Perubahan Bidang Kuasa 12
7.2.3. Forensik / *Data Seizure* 13
7.2.4. Kebergantungan 14

7.2.5. *Multi-Tenancy* 14
7.2.6. Ancaman Dari Sumber Dalaman CSP 15
7.2.7. *Vendor Lock-in* 16
7.2.8. Privasi 16
8. TADBIR URUS 18
8.1.1. Pengurusan Risiko 18
9. PEMATUHAN PENGURUSAN MAKLUMAT RAHSIA RASMI 19
9.1.1. Klasifikasi Maklumat 19
9.1.2. Bidang Kuasa 20
9.1.3. Kawalan Pengguna 20
9.1.4. Khidmat Nasihat Undang-Undang 20
9.1.5. Kaedah Penentuan Residensi Data 21
9.1.6. Pengurusan dan Kawalan Kriptografi 21
9.1.7. Pengecualian Residensi Data 22
10. PENGURUSAN KONTRAK DAN TERMA KESELAMATAN 22
10.1. *Due Diligence* 22
10.2. *Service Level Agreement* (SLA) 23
10.3. Hak Milik Data (Data Ownership) 23
10.4. Privasi 24
10.5. Audit 24
10.6. Pampasan (*Compensation*) 25
10.7. Liabiliti 25
10.8. Hak Mencapai Elemen 25
10.9. Pelucutan Perkhidmatan (Exit Process) 25
11. KEPENTINGAN MELINDUNGI MAKLUMAT DALAM PERSEKITARAN ICT . 26
12. KAEDAH PERLINDUNGAN DATA DAN MAKLUMAT 27
12.2.1. Enkripsi 27
12.2.2. Pengasingan 28
12.2.3. Pengurusan Akses dan Identiti 28
12.2.4. Perisian dan Aplikasi Keselamatan 30
12.2.5. Penilaian Tahap Keselamatan 31
12.2.6. Sanitasi Data 32
12.2.7. Ketirisan Data / Maklumat 33
13. KAWALAN KESELAMATAN FIZIKAL PUSAT DATA DAN INFRASTRUKTUR ICT 34

13.2.1. Penilaian Keselamatan 34
13.2.2. Kawasan Terperingkat 34
13.2.3. Pematuhan dan Pensijilan Keselamatan 35
13.2.4. Tapisan Keselamatan 35
13.2.5. Validasi Keselamatan Rahsia Rasmi 36
13.2.6. Sokongan 36
13.2.7. Notifikasi 36
14. PENGURUSAN INSIDEN 36
15. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 37
16. KEBOLEHSEDIAAN DAN SANDARAN DATA 37
17. KESIMPULAN 38
18. RUJUKAN 38
LAMPIRAN 1 40
LAMPIRAN 2 41

KAWALAN VERSI DOKUMEN

Jadual di bawah mengandungi perubahan yang dikemaskini di dalam dokumen garis panduan versi 2.0 ini. Kemaskini ini meliputi pembetulan, penjelasan tambahan atau lain-lain perubahan minor atau major ke atas kandungan yang boleh dikategorikan sebagai editorial dan substantif. Butiran perubahan adalah seperti berikut;

TARIKH	JENIS	RINGKASAN PINDAAN	MUKA SURAT
6 Mei 2024	Editorial	Perubahan struktur nombor dan format keseluruhan dokumen	Semua muka surat
6 Mei 2024	Substantif	Perubahan paparan utama dan versi dokumen kepada versi 2.0 berkuat kuasa pada tarikh dikeluarkan	-
6 Mei 2024	Substantif	Tambahan baharu Kawalan Versi Dokumen	v
6 Mei 2024	Substantif	Akronim dan Definisi; *Tambahan baharu definisi Data Peribadi*	viii
6 Mei 2024	Substantif	Akronim dan Definisi; *Tambahan baharu definisi Data Sovereignty*	viii
6 Mei 2024	Substantif	Akronim dan Definisi; *Tambahan baharu definisi Failover*	viii
6 Mei 2024	Editorial	Akronim dan Definisi; *Kemaskini Data Residency kepada Residensi Data*	ix
6 Mei 2024	Substantif	Kemaskini Perkara 4: Klasifikasi Maklumat Atau Data *Kemaskini perenggan 4.1.1 (a)*	3
6 Mei 2024	Substantif	Kemaskini Perkara 4: Klasifikasi Maklumat Atau Data *Kemaskini perenggan 4.1.1 (b)*	4
6 Mei 2024	Substantif	Kemaskini Perkara 4: Klasifikasi Maklumat Atau Data *Kemaskini: 4.1.3 Data Terkawal / Sensitif*	4
6 Mei 2024	Substantif	Kemaskini Perkara 6: Penentuan Model Pelaksanaan Pengkomputeran Awan Bagi Perkhidmatan Awam *Tambahan perenggan baharu: 6.2*	8
6 Mei 2024	Substantif	Kemaskini Perkara 9: Pematuhan Pengurusan Maklumat Rahsia Rasmi	19

		Kemaskini perenggan 9.1	
6 Mei 2024	Substantif	Kemaskini Perkara 9: Pematuhan Pengurusan Maklumat Rahsia Rasmi *Tambahan perenggan baharu: Perenggan 9.1.5 Kaedah Penentuan Residensi Data*	21
6 Mei 2024	Substantif	Kemaskini Perkara 9: Pematuhan Pengurusan Maklumat Rahsia Rasmi *Tambahan perenggan baharu: 9.1.6 Pengurusan dan Kawalan Kriptografi*	21
6 Mei 2024	Substantif	Kemaskini Perkara 9: Pematuhan Pengurusan Maklumat Rahsia Rasmi *Tambahan perenggan baharu: 9.1.7 Pengecualian Residensi Data*	22
6 Mei 2024	Substantif	Kemaskini Perkara 10: Pengurusan Kontrak Dan Terma Keselamatan *Tambahan perenggan baharu 10.1.2*	22
6 Mei 2024	Substantif	Kemaskini Perkara 12: Kaedah Perlindungan Data Dan Maklumat *Tambahan perenggan baharu: 12.2*	27
6 Mei 2024	Substantif	Kemaskini Perkara 12: Kaedah Perlindungan Data Dan Maklumat *Kemaskini Perenggan 12.2.6 Sanitasi Data* 1. *Kemaskini perkara (a)* 2. *Kemaskini perkara (e)* 3. *Tambahan perenggan baharu perkara (f)*	32 & 33
6 Mei 2024	Substantif	Kemaskini Perkara 13: Kawalan Keselamatan Fizikal Pusat Data Dan Infrastruktur ICT di bawah *Kemaskini perenggan 13.2.3 Pematuhan dan Pensjilan Keselamatan*	35
6 Mei 2024	Substantif	Kemaskini Perkara 16: Kebolehsediaan Dan Sandaran Data *Tambahan perenggan baharu 16.3*	38
6 Mei 2024	Editorial	Kemaskini Perkara 18: Rujukan	38
6 Mei 2024	Substantif	Kemaskini Lampiran 1	40
6 Mei 2024	Substantif	Tambahan baharu Lampiran 2	41

AKRONIM DAN DEFINISI

TERMA	AKRONIM DAN DEFINISI
CSP	Pihak penyedia perkhidmatan pengkomputeran awan / Cloud Services Provider
Data Peribadi	Apa-apa maklumat yang digunakan di dalam transaksi komersial yang berhubungan secara langsung atau tidak langsung dengan seseorang subjek data yang dikenalpasti daripada maklumat tersebut. Data tersebut boleh direkodkan, sama ada secara manual atau elektronik meliputi perkara-perkara objektif dan subjektif tanpa mengira sumber maklumat itu diperolehi meliputi maklumat asas (contohnya nama, alamat dan nombor kad pengenalan) sehinggalah ke maklumat sensitif (contohnya rekod perubatan dan tahap kesihatan) atau apa-apa informasi lain yang ditetapkan menteri di bawah Akta Perlindungan Data Peribadi 2010 [*Akta 709*].
Data Sovereignty	Apa-apa data yang dijana atau diperoleh di dalam negara adalah tertakluk kepada undang-undang dan peraturan di bawah bidang kuasa Kerajaan Malaysia serta tadbir urus yang berkaitan.
Failover	Keupayaan untuk memindahkan sumber ICT secara automatik (tanpa penglibatan manusia) kepada sistem tunggu sedia (standby) apabila berlaku kegagalan atau sesuatu peristiwa di luar kebiasaan (abnormal) pada sistem utama.
HTTP	*HyperText Transfer Protocol*
IPSec	*Internet Protocol Security*
Jabatan	Sesebuah Kementerian, Jabatan Kerajaan, Badan Berkanun, Kerajaan Tempatan dan agensi lain yang kepadanya Akta 88 terpakai.
MFA	Pengesahan pelbagai faktor / *Multi Factor Authentication*
PDA	Pelbagai peranti mudah alih yang berfungsi sebagai pengurus maklumat peribadi / *Personal Digital Assistant*

PII	Maklumat Pengenalan Peribadi / *Personally Identifiable Information*
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan Negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberikan keuntungan besar kepada sesebuah kuasa asing hendaklah diperingkatkan sebagai "Rahsia".
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan sebagai "Rahsia Besar"
Residensi Data	Merujuk kepada di mana sesuatu perniagaan, badan industri atau Kerajaan menentukan data disimpan di lokasi fizikal secara geografi yang mereka pilih, atas beberapa alasan seperti keperluan pengawalseliaan dan pematuhan polisi.
SFTP	*Secure File Transfer Protocol*
Snapshot	Kaedah untuk menyalin memori dan cakera pelayan yang sedang digunakan (running server).
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan sebagai "Sulit".
SSL	*Secure Sockets Layer*
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan sebagai "Rahsia Besar", "Rahsia" atau "Sulit" tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan sebagai "Terhad".

TLS	*Transport Layer Security*
VPN	*Virtual Private Network*
Virtualization	Proses untuk mewujudkan/mencipta perwakilan sesuatu berasaskan perisian, atau maya seperti aplikasi maya, pelayan, storan dan rangkaian. Dalam pengkomputeran awan, ia merupakan teknologi penting yang membolehkan sistem maklumat diperoleh (abstract) daripada *underlying hardware* dengan menggunakan *hypervisor* iaitu perisian yang membenarkan hos pelayan menjalankan pelbagai sistem operasi (multiple guest operating system) dalam satu-satu masa.

GARIS PANDUAN PENGURUSAN KESELAMATAN MAKLUMAT MELALUI PENGKOMPUTERAN AWAN (CLOUD COMPUTING) DALAM PERKHIDMATAN AWAM

1. PENGENALAN

1.1. Pengkomputeran awan (cloud computing) merupakan model yang membolehkan capaian rangkaian kepada himpunan sumber pengkomputeran (contoh: rangkaian, pelayan, storan, aplikasi dan perkhidmatan) dengan mudah dan cepat melalui urusan interaksi dan usaha pengurusan yang minimum dengan pembekal perkhidmatan. Perkhidmatan pengkomputeran awan yang fleksibel dan elastik (mengikut keperluan dan permintaan pengguna) dilihat mampu menawarkan penjimatan kos di samping meningkatkan kecekapan perkhidmatan ICT. Walau bagaimanapun, penggunaan perkhidmatan tersebut dalam melaksanakan urusan am dan urusan fungsian sesebuah Jabatan memberi cabaran baharu berbanding dengan pendekatan konvensional. Cabaran tersebut termasuklah keselamatan, perubahan pengurusan, saling bergantung (interoperability) dan aspek perundangan yang perlu diambil kira sebelum ianya diterima pakai dan dilaksanakan. Keselamatan maklumat dan data Kerajaan yang dikendalikan dalam pengkomputeran awan terutama sekali yang melibatkan rahsia rasmi Kerajaan hendaklah diurus dan dikawal dengan sebaiknya bagi mengelakkan berlakunya ketirisan maklumat Kerajaan.

2. TUJUAN

2.1. Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam bertujuan:

i. sebagai rujukan kepada Jabatan mengenai pengurusan keselamatan perlindungan berhubung perkara rasmi dan rahsia rasmi Kerajaan dalam persekitaran pengkomputeran awan;

ii. membantu Jabatan memahami pengurusan rahsia rasmi dalam pengkomputeran awan selaras dengan peruntukan undang-undang semasa seperti di bawah Akta Rahsia Rasmi 1972 [*Akta 88*] dan Arahan Keselamatan (Semakan dan Pindaan 2017); dan

iii. menerangkan langkah-langkah kawalan mitigasi yang wajar dan efektif berdasarkan kepada pengolahan risiko yang telah dikenal pasti ke atas aset ICT yang dipindahkan atau digunakan dalam perkhidmatan pengkomputeran awan.

3. PELAKSANAAN PENGKOMPUTERAN AWAN DI DALAM PERKHIDMATAN AWAM

3.1. Pengkomputeran awan adalah merujuk kepada paradigma atau model pengkomputeran yang membolehkan capaian rangkaian kepada himpunan sumber pengkomputeran yang fleksibel dan elastik dengan cara perkongsian sumber bersama, sama ada secara fizikal atau maya dengan keupayaan pembekalan secara layan diri atau pengurusan oleh pihak ketiga mengikut permintaan pengguna.

3.2. Pengurusan rahsia rasmi dalam pengkomputeran awan di dalam perkhidmatan awam hendaklah mematuhi perenggan 139, Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut:

Penggunaan pengkomputeran awan (cloud computing) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

3.3. Secara asasnya maksud pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan adalah perkhidmatan pengkomputeran awan yang dimiliki, diuruskan atau dikendalikan oleh pihak Kerajaan sendiri

berdasarkan kepada prinsip, penilaian dan keperluan keselamatan siber secara komprehensif dan strategik melibatkan teknologi, manusia dan proses. Ia bertujuan agar perkhidmatan pengkomputeran awan tersebut memenuhi objektif keselamatan, hala tuju bisnes serta keperluan peraturan dan undang-undang yang berkuat kuasa.

4. KLASIFIKASI MAKLUMAT ATAU DATA

4.1. Akta Rahsia Rasmi 1972 [*Akta 88*] dan Arahan Keselamatan (Semakan dan Pindaan 2017) secara asasnya menyatakan beberapa *pre-defined rules* di dalam proses pengelasan maklumat berdasarkan kepada nilai, impak dan sensitiviti. Bagi memberi kefahaman awal, antara kategori maklumat dan tahap pengelasan maklumat yang sering diuruskan oleh Jabatan di bawah perkhidmatan awam adalah seperti berikut:

4.1.1. **Rasmi**

(a) Rasmi adalah berhubungan dengan perkhidmatan awam. Maklumat rasmi yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana Jabatan Kerajaan semasa menjalankan urusan rasmi. Ianya juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara Malaysia. Berikut adalah beberapa contoh bagi maklumat rasmi Kerajaan:

i. Kewangan;
ii. Perubatan;
iii. Kesihatan;
iv. Akademik;
v. Percukaian;
vi. Perjanjian/Kontrak;
vii. Data Kajian; dan
viii. Maklumat Pengenalan Peribadi (*Personally Identifiable Information- PII*).

(b) Maklumat **Rasmi** seperti di atas juga boleh menjadi rahsia rasmi sekiranya pemula (pemilik data) membuat tafsiran risiko yang sepadan dengan salah satu peringkat keselamatan rahsia rasmi yang dimaksudkan. Pelepasan dan pemilikan perkara rasmi tanpa kebenaran daripada pemula juga menjadi satu kesalahan seperti mana tertakluk di bawah undang-undang dan peraturan-peraturan semasa. Sebagai contoh seksyen 203A, Kanun Keseksaan [*Akta 574*].

4.1.2. **Data Terbuka (*Open Data*)**

Data Terbuka adalah maklumat rasmi yang telah dibuat saringan dan pengesahan di peringkat pemula data untuk bebas digunakan, dikongsi serta digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Jabatan hendaklah mematuhi pekeliling berhubung data terbuka yang sedang berkuat kuasa**.**

4.1.3. **Data Terkawal / Sensitif**

Data Terkawal / Sensitif adalah data yang mempunyai kawalan tertentu di bawah Akta atau Peraturan selain daripada Akta 88. Selain itu, data yang mempunyai nilai muka atau sensitif sifatnya yang ditentukan sendiri oleh Jabatan menurut pandangannya.

4.1.4. **Rahsia Rasmi**

Rahsia Rasmi mempunyai erti seperti yang diberikan kepada takrifan “rahsia rasmi” di bawah Akta Rahsia Rasmi 1972 [*Akta 88*] iaitu *“apa-apa suratan yang dinyatakan dalam Jadual dan apa-apa maklumat dan bahan yang berhubungan dengannya dan termasuklah apa-apa suratan rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad”, mengikut mana-mana yang berkenaan, oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B”.*

5. CIRI–CIRI ASAS DAN MODEL PERKHIDMATAN PENGKOMPUTERAN AWAN

5.1. Ciri-Ciri Asas Pengkomputeran Awan

5.1.1. Permintaan Secara Layan Diri (On Demand Self-Service)

Pengguna boleh melakukan semua proses penetapan keperluan pengkomputeran awan yang dikehendaki, contohnya storan, rangkaian, aplikasi tanpa intervensi manusia daripada penyedia perkhidmatan.

5.1.2. Akses Rangkaian Yang Meluas (Broad Network Access)

Perkhidmatan yang disediakan dalam rangkaian yang tersedia daripada pelbagai lokasi dan melalui pelbagai peranti sebagai contoh desktop, komputer riba, PDA, telefon pintar dan sebagainya.

5.1.3. *Resource Pooling*

Sumber pengkomputeran dihimpunkan untuk memberi perkhidmatan kepada pelbagai pengguna menggunakan model *multi-tenant* dengan sumber fizikal dan maya diperuntukkan secara dinamik mengikut permintaan pengguna. Contoh sumber termasuklah storan, pemprosesan, memori dan rangkaian jalur lebar.

5.1.4. Keanjalan Pantas (Rapid Elasticity)

Kebolehan skala perkhidmatan ditambah atau dikurangkan secara dinamik mengikut keperluan.

5.1.5. Measured *Service*

Sistem berupaya mengukur (metering) nilai perkhidmatan (kos dan sumber ICT) yang diberikan kepada pengguna yang bersesuaian

dengan jenis perkhidmatan (contoh: storan, *bandwidth* atau jumlah akaun pengguna yang aktif). Pengukuran tahap *service-level agreement* (SLA) yang ditawarkan *Cloud Service Provider* (CSP) hendaklah selaras dengan keperluan perkhidmatan teras dan persetujuan pemegang taruh Jabatan.

5.2. Model Perkhidmatan Pengkomputeran Awan

5.2.1. Perisian Sebagai Perkhidmatan (Software-as-a-Service -SaaS)

(a) Model perkhidmatan yang membenarkan Jabatan untuk menggunakan aplikasi dan kemudahan infrastruktur pengkomputeran awan yang dibangunkan atau disediakan oleh penyedia perkhidmatan. Aplikasi tersebut boleh diakses oleh peranti pengguna melalui pelbagai saluran (web browser, web-based email). Jabatan hanya dibenarkan membuat konfigurasi asas terhadap aplikasi manakala kemudahan infrastruktur pengkomputeran seperti rangkaian, pelayan, sistem pengoperasian, storan dan konfigurasi aplikasi diuruskan oleh penyedia perkhidmatan.

(b) Objektif utama model perkhidmatan ini adalah bagi mengurangkan kos operasi, perolehan perkakasan dan perisian, kos penyelenggaraan aplikasi atau kos penyelenggaraan infrastruktur pengkomputeran awan.

(c) Peruntukan keselamatan terhadap aplikasi dan infrastruktur pengkomputeran awan adalah sepenuhnya di bawah tanggungjawab penyedia perkhidmatan.

5.2.2. Platform Sebagai Perkhidmatan (Platform-as-a-Services - PaaS)

(a) Model perkhidmatan yang menyediakan satu platform kepada Jabatan untuk membangunkan sesebuah aplikasi atau perisian, diuji dan digunapakai (deployed) di dalam persekitaran pengkomputeran awan. Kitar hayat pembangunan aplikasi atau perisian menggunakan

peralatan dan kaedah pengaturcaraan tertentu (contoh: programming language, libraries) yang telah disediakan oleh penyedia perkhidmatan.

(b) Objektif utama model perkhidmatan ini bertujuan mengurangkan kos operasi, memudahkan proses pembelian, penempatan dan pengurusan komponen perkakasan dan platform perisian, termasuklah sebarang keperluan di dalam pembangunan program dan pangkalan data.

(c) Peruntukan keselamatan bagi model perkhidmatan ini adalah **di bawah tanggungjawab penyedia perkhidmatan dan Jabatan**.

5.2.3. **Infrastruktur Sebagai Perkhidmatan (Infrastructure-as-a-Services - IaaS)**

(a) Model perkhidmatan yang menyediakan sumber asas pengkomputeran seperti storan, rangkaian, pelayan secara maya bagi menyokong operasi aplikasi atau perisian Jabatan. Model perkhidmatan ini hanya membenarkan Jabatan mengurus dan mengawal sistem pengoperasian (OS), storan, aplikasi dan komponen rangkaian tertentu (contoh: firewall). IaaS merupakan sebuah perkhidmatan yang disediakan di mana infrastruktur asas pengkomputeran seperti *server*, sistem operasi dan peralatan rangkaian disediakan mengikut permintaan atau keperluan Jabatan.

(b) Objektif utama dalam pemilihan model perkhidmatan IaaS adalah untuk penjimatan kos yang perlu dikeluarkan oleh Jabatan dalam pembelian peralatan pengkomputeran, penyewaan lokasi serta penyelenggaraan terhadap infrastruktur (perkakasan dan perisian).

(c) Peruntukan keselamatan **selain daripada infrastruktur asas pengkomputeran** adalah **di bawah tanggungjawab Jabatan.**

6. PENENTUAN MODEL PELAKSANAAN PENGKOMPUTERAN AWAN BAGI PERKHIDMATAN AWAM

6.1. Penentuan model pelaksanaan pengkomputeran awan yang ingin dipilih adalah berdasarkan kepada klasifikasi maklumat yang telah dibuat oleh pemilik data (data/business owner) bagi sesebuah Jabatan. Klasifikasi maklumat ini dinilai dari sudut implikasi kepada keselamatan, pertahanan, fungsi dan pentadbiran kerajaan, kepentingan dan martabat negara.

6.2. Penentuan model pelaksanaan pengkomputeran awan adalah seperti berikut:

6.2.1. ***Private Cloud***

(a) Infrastruktur awan yang disediakan **khusus bagi kegunaan** Jabatan. Ianya mungkin dimiliki, diuruskan dan dikendalikan oleh Jabatan, pihak ketiga, atau kedua-duanya sekali dan ianya wujud di dalam atau di luar premis.

(b) Pihak ketiga di sini merujuk kepada entiti yang memberi perkhidmatan kepada pihak Jabatan untuk menguruskan pengkomputeran awan miliknya.

(c) Model ini sesuai digunakan bagi semua kategori maklumat atau data kerajaan. Walau bagaimanapun, bagi klasifikasi maklumat tertentu ia perlu memenuhi **pra-syarat** seperti berikut:

MAKLUMAT RAHSIA RASMI BAGI PERINGKAT TERHAD DAN SULIT

(i) Maklumat rahsia rasmi berperingkat TERHAD dan SULIT termasuk sistem aplikasinya boleh dikendalikan secara *private cloud* sekiranya perkhidmatan tersebut dibangunkan dan dibenarkan oleh pihak kerajaan.

(ii) Maklumat rahsia rasmi berhubung perkara **dalam Jadual Akta 88** hendaklah dihoskan di dalam premis Jabatan (on-premise) manakala maklumat rahsia rasmi **luar Jadual** dibenarkan di dalam premis atau bukan premis Jabatan (off-premise).

(iii) Perkhidmatan *private cloud* secara *on-premise* adalah merujuk kepada pengkomputeran awan yang dibangunkan di premis Jabatan itu sendiri atau pun melalui Pusat Data Sektor Awam (PDSA) Kerajaan. Jabatan perlu merujuk kepada pihak Jabatan Digital Negara bagi menggunakan perkhidmatan yang disediakan oleh PDSA. PDSA menyediakan fasiliti pusat data dan infrastruktur ICT untuk guna sama agensi / jabatan secara berpusat. Bagi perkhidmatan yang ditawarkan secara *off-premise,* lokaliti pengkomputeran awan tersebut berada di bawah kawalan perundangan dan bidang kuasa Kerajaan Malaysia.

MAKLUMAT RAHSIA RASMI BAGI PERINGKAT RAHSIA DAN RAHSIA BESAR

(i) Pengurusan maklumat rahsia rasmi berperingkat RAHSIA dan RAHSIA BESAR dalam persekitaran pengkomputeran awan hendaklah terlebih dahulu dinilai dengan teliti dan berhati-hati dari sudut risiko, impak dan ancaman terhadap keselamatan negara sekiranya dilaksanakan. Kesilapan dalam pengendalian maklumat rahsia rasmi berperingkat RAHSIA dan RAHSIA BESAR dalam pengkomputeran awan akan memberi implikasi yang besar kepada keselamatan negara.

(ii) Sebarang cadangan pengurusan maklumat rahsia rasmi berperingkat RAHSIA dan RAHSIA BESAR melalui pengkomputeran awan hendaklah merujuk terlebih dahulu ke Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) bagi khidmat nasihat dan penilaian risiko keselamatan.

MAKLUMAT RASMI

(i) Maklumat rasmi termasuk sistem aplikasinya boleh dikendalikan di *private cloud* yang dibangunkan dan/atau dibenarkan oleh pihak kerajaan sama ada di *on-premise* atau *off-premise*.

6.2.2. ***Public Cloud***

Infrastruktur pengkomputeran awan yang disediakan untuk **kegunaan awam**. Ia mungkin dimiliki, diuruskan dan dikendalikan oleh sesebuah entiti perniagaan, akademik atau agensi kerajaan yang wujud di dalam premis penyedia perkhidmatan (Cloud Services Provider, CSP). Penggunaan model ini adalah sesuai digunakan bagi data terbuka dan maklumat rasmi yang tidak sensitif.

6.2.3. ***Hybrid Cloud***

Infrastruktur pengkomputeran awan yang terdiri daripada **dua atau lebih gabungan model pengkomputeran awan** (private atau public) yang mewujudkan satu entiti baharu yang terikat antara satu sama lain melalui perjanjian atau kerjasama yang dipersetujui. Model ini dibenarkan bagi maklumat rasmi. Ia juga dibenarkan untuk maklumat rahsia rasmi bagi peringkat TERHAD dan SULIT sahaja dengan mengambil kira lokaliti kedua-dua pengkomputeran awan tersebut berada di bawah kawalan perundangan dan bidang kuasa Kerajaan Malaysia.

Jadual Matrix Pelaksanaan Pengkomputeran Awan Dalam Perkhidmatan Awam mengikut klasifikasi maklumat boleh merujuk di **LAMPIRAN 1**.

7. RISIKO KESELAMATAN YANG PERLU DIPERTIMBANGKAN

7.1. Pengkomputeran awan merupakan medium untuk memudahkan penyampaian perkhidmatan awam yang lebih efektif dan ekonomi. Walau bagaimanapun, ia mempunyai impak dan implikasi negatif sekiranya dilaksanakan tanpa mematuhi aspek keselamatan terhadap perlindungan maklumat. Selain itu, menyerahkan ketersediaan dan keselamatan data, aplikasi dan infrastruktur ICT kepada pihak ketiga boleh mengundang dan meningkatkan risiko keselamatan.

7.2. Jabatan Kerajaan yang ingin melaksanakan pengkomputeran awan hendaklah memberi pertimbangan ke atas beberapa faktor semasa membuat pemilihan CSP seperti berikut:

7.2.1. **Kedaulatan Data (Data Sovereignty)**

(a) Penggunaan perkhidmatan pengkomputeran awan yang berada di luar Malaysia dalam mengendalikan maklumat Kerajaan boleh mendatangkan bahaya kepada keselamatan dan kedaulatan data negara. Data yang disimpan, diproses dan dipindahkan menerusi perkhidmatan tersebut mungkin tertakluk kepada peruntukan undang-undang negara berkenaan serta berada di luar kawalan dan bidang kuasa Kerajaan Malaysia.

(b) Ini termasuklah bagi mana-mana pihak pembekal yang berdaftar dan mempunyai Ibu Pejabat (Headquarters) di luar negara yang menjalankan operasi perniagaannya di Malaysia. Faktor lain yang perlu diambil kira sekiranya pihak CSP ada menggunakan sumber luar atau bergantung kepada pihak ketiga untuk menyampaikan perkhidmatannya kepada pelanggan. Oleh yang demikian, Jabatan hendaklah mengenal pasti sumber asal (source of origin) perkhidmatan pengkomputeran awan tersebut dengan memahami aliran dan residensi data bagi memastikan tiada sebarang kuasa asing lain yang

boleh akses maklumat dan data strategik negara tanpa pengetahuan dan kebenaran.

(c) Kedaulatan data (data sovereignty) perlu merujuk kepada keperluan undang-undang atau pengawalseliaan yang dikenakan ke atas data berdasarkan wilayah atau negara di mana ia berada secara fizikal. Kedaulatan data perlu menjadi keperluan utama di dalam penggunaan pengkomputeran awan oleh Jabatan dengan mengenal pasti perkara berikut:

i. Tadbir urus dan pemegang taruh data di Jabatan;
ii. Keselamatan data;
iii. Kedudukan geografi dan penempatan fizikal data;
iv. Peraturan, prosedur dan perundangan;
v. Risiko keselamatan;
vi. Klasifikasi data;
vii. Hak milik data; dan
viii. Aliran data.

(d) Bagi pengendalian rahsia rasmi Kerajaan, Jabatan hendaklah diberi kebenaran untuk menentukan di mana data disimpan dan diproses.

7.2.2. **Risiko Daripada Perubahan Bidang Kuasa**

(a) Jabatan hendaklah memahami kehendak undang-undang, hak kontraktual dan pertindihan bidang kuasa berhubung dengan tempat penyimpanan dan pemprosesan data secara logikal atau fizikal. Data Jabatan mungkin disimpan di dalam beberapa wilayah yang mempunyai bidang kuasa yang berbeza, ada di antaranya di negara berisiko tinggi.

(b) Sebagai contoh, pusat data CSP yang berada dan beroperasi di dalam negara yang mengamalkan autokrasi, tidak mempunyai tadbir urus undang-undang yang baik atau negara yang tidak menghormati perjanjian antarabangsa yang boleh menyebabkan pusat data tersebut di akses dan berlakunya pelepasan data dan sistem ICT tanpa keizinan oleh pemilik asal.

7.2.3. **Forensik / *Data Seizure***

(a) Agensi penguatkuasaan undang-undang (law enforcement agency, LEA) mempunyai kuasa untuk mengakses komunikasi dan maklumat bagi tujuan penguatkuasaan dan penyiasatan (data seizure) sekiranya berlaku pelanggaran undang-undang. Dalam kes tertentu, undang-undang tersebut juga memberi kebenaran agensi penguatkuasaan asing (international law enforcement) untuk mengakses maklumat sama ada di dalam ataupun di luar negara.

(b) *Bit-by*-bit *imaging* atau salinan data bagi tujuan forensik dalam persekitaran pengkomputeran awan pula kebiasaannya sukar untuk dilaksanakan. Pihak penyedia perkhidmatan terikat dengan polisi keselamatan agar tidak membiarkan perkakasan dan perisiannya diakses oleh pengguna terutamanya dalam persekitaran *multi-tenant* dimana pelanggan mungkin mempunyai akses ke atas sumber di antara satu sama lain.

(c) Selain itu, struktur data dalam teknologi *virtualization* juga menyukarkan proses forensik dan analisis dilakukan. Dalam konfigurasi tertentu, data mungkin tidak dapat diperoleh sama sekali dan siasatan mungkin gagal dijalankan dengan berkesan.

7.2.4. **Kebergantungan**

(a) Pihak ketiga mungkin terlibat di dalam sesuatu proses atau perkhidmatan yang disediakan kepada pengguna. Kebergantungan pihak CSP kepada pihak ketiga tersebut boleh menyebabkan risiko keselamatan yang tidak diketahui dan disedari.

(b) Perkhidmatan ini juga bergantung dengan pengurusan rantaian bekalan (supply chain management) yang perlu dilihat secara holistik bagi memastikan peraturan, polisi dan amalan baik dalam keselamatan diaplikasikan oleh semua pihak yang terlibat.

7.2.5. ***Multi-Tenancy***

(a) Dalam model pelaksanaan pengkomputeran awan tertentu ia membenarkan pengguna yang terdiri daripada pelbagai entiti (multi-tenancy) berkongsi sumber ICT yang sama (resource pooling).

(b) Elemen ini menjadikan perkhidmatan pengkomputeran awan menjadi pilihan kepada Jabatan untuk mengurangkan kos operasi dan perolehan aset ICT berbanding dengan model biasa.

(c) Risiko berkaitan dengan *multi-tenancy* yang perlu diketahui oleh Jabatan kebiasaannya adalah melalui infrastruktur *virtualization* atau *data commingling*.

(d) Dalam persekitaran *virtualization*, serangan kod jahat boleh berlaku sekiranya wujud kerentanan keselamatan dalam *hypervisor* dan mengakibatkan maklumat Jabatan diakses oleh pihak lain. Sebagai contoh, serangan siber boleh dilakukan melalui *'guest-to-host'* atau *'guest-to-guest'* oleh mereka yang sudah mempunyai akses terhadap perkhidmatan tersebut.

(e) Jabatan boleh melakukan *snapshot* pada masa-masa tertentu untuk tujuan salinan sandaran dan *redundancy* dengan lebih mudah melalui teknologi *virtualization*. Namun begitu, jika salinan tersebut (actual copy) tidak dilindungi dengan betul, maklumat yang disimpan dalam mesin maya (virtual machine's local drives) mungkin boleh diakses oleh pihak lain. Ini juga termasuklah semua data dan kunci enkripsi yang disimpan dalam memori berkenaan.

(f) Dalam model perkhidmatan IaaS dan PaaS, pelanggan yang tidak melaksanakan amalan baik dalam pengurusan dan kawalan keselamatan boleh menjejaskan tahap keselamatan CSP ke tahap yang paling berisiko (the lowest common denominator problem). Sebagai contoh, pelanggan yang tidak membuat pengukuhan sistem operasi dan aplikasinya boleh mengakibatkan berlakunya situasi demikian jika tiada kawalan bersesuaian dilakukan untuk mengasingkan rangkaian dan mesin maya setiap pelanggan.

(g) Sementara itu, permintaan secara layan diri dalam perkhidmatan pengkomputeran awan memudahkan pengguna membuat pendaftaran untuk melanggani perkhidmatan melalui *Cloud Management Portal* (CMP) yang disediakan oleh pihak CSP. Bagaimanapun kemudahan ini boleh dimanipulasi oleh pihak tidak bertanggungjawab untuk mendaftar dan menggunakan perkhidmatan tersebut dan seterusnya melakukan aktiviti yang tidak sah dan berbahaya kepada pengguna yang lain.

7.2.6. **Ancaman Dari Sumber Dalaman CSP**

(a) Jabatan yang merancang untuk menggunakan perkhidmatan pengkomputeran awan hendaklah menilai risiko sekiranya terdapat kemungkinan maklumat yang disimpan dalam fasiliti pihak penyedia di akses tanpa kebenaran sama ada oleh pekerja, kontraktor atau mana-mana pihak ketiga (supply chain) yang lain.

(b) Jabatan dikhuatiri mungkin tidak mempunyai keupayaan untuk mengukur tahap keselamatan seterusnya membuat pengesahan keberkesanan kawalan dan prosedur seperti yang ditawarkan oleh pihak CSP.

(c) Sebagai contoh, tahap jaminan keselamatan adalah berbeza bergantung kepada lokasi fizikal CSP dan kakitangannya. CSP tempatan tertakluk kepada syarat keselamatan yang perlu dilaksanakan seperti mengenakan tapisan keselamatan kepada semua pekerja dan kakitangan yang mengendalikan maklumat strategik Kerajaan. Bagaimanapun prosedur ini mungkin tidak dapat dilaksanakan jika perkhidmatan pengkomputeran awan tersebut disediakan dari luar negara.

7.2.7. ***Vendor Lock-in***

(a) *Vendor lock-in* merupakan satu keadaan di mana pihak Jabatan mengalami kesukaran untuk memindahkan perkhidmatan atau data sedia ada kepada CSP atau pihak lain. Ia mungkin disebabkan oleh format data atau infrastruktur CSP yang berbeza di antara satu sama lain mahupun pihak CSP semasa gagal memberikan kerjasama yang sepatutnya.

(b) Jabatan *perlu* memastikan isu ini diberi perhatian dan tindakan sewajarnya seperti menyediakan pasukan pakar (subject matter expert, SME) yang boleh memberi sokongan teknikal sewaktu proses transisi dan migrasi pengkomputeran awan dilakukan.

7.2.8. **Privasi**

(a) Privasi merujuk kepada hak jabatan atau individu yang bertindak bagi pihak jabatan atau dirinya, untuk menentukan sejauh mana ia akan

berinteraksi dengan persekitarannya. Ini termasuk sejauh mana ia sanggup berkongsi maklumat atau data antara Jabatan atau entiti lain.

(b) Di dalam peringkat mengenal pasti risiko, Jabatan perlu memastikan cadangan pengkomputeran awan tidak melibatkan perlanggaran privasi data kepada Jabatan. Kawalan data boleh dipertingkatkan melalui proses data *anonymization* seperti data masking atau data scrambling bagi memastikan data sebenar tidak terdedah tetapi masih boleh di analisa, diproses dan diguna oleh pihak CSP mengikut keperluan pengguna. Jabatan terlebih dahulu boleh melaksanakan *proof-of-concept* (PoC) bagi memastikan penyelesaian teknikal yang diperlukan menepati objektif pelaksanaannya, Data yang telah melalui proses *anonymization* tersebut boleh dipindahkan dan di proses di dalam fasiliti CSP sementara data asal yang sensitif dan terkawal ditempatkan di bawah jagaan Jabatan bagi tujuan pemadanan.

(c) Skop keselamatan adalah termasuk model pengkomputeran awan yang diuruskan oleh pihak ketiga di premis kerajaan (on-premises) atau milik Jabatan di premis bukan Kerajaan.

8. TADBIR URUS

8.1. Struktur tadbir urus hendaklah dikenal pasti dan diwujudkan untuk merancang, mengurus dan mengawal polisi serta fungsi yang berkaitan dengan keselamatan maklumat dalam pengurusan pengkomputeran awan. Tadbir urus yang diwujudkan hendaklah mengambil kira perkara-perkara seperti berikut:

8.1.1. **Pengurusan Risiko**

(a) pengurusan risiko dalam pengkomputeran awan antara cabaran yang perlu diberi perhatian oleh Jabatan memandangkan sebahagian besar sumber pengkomputeran adalah di bawah kawalan oleh pihak CSP dan terdapat kemungkinan ia tidak boleh diakses oleh Jabatan. Risiko perlu dinilai berdasarkan kepada kawalan teknikal, pengurusan, pengoperasian dan langkah-langkah yang diambil untuk meminimumkan risiko ke tahap yang boleh diterima; dan

(b) risiko penggunaan pengkomputeran awan yang melibatkan maklumat rasmi dan rahsia rasmi Kerajaan hendaklah ditentukan dan diputuskan oleh pemegang taruh (stakeholder) di Jabatan berdasarkan hasil penilaian risiko yang telah dibuat. Jabatan hendaklah mengenal pasti struktur tadbir urus pengurusan risiko keselamatan perlindungan terhadap aset ICT yang menggunakan perkhidmatan pengkomputeran awan. Tadbir urus ini bertanggungjawab seperti berikut:

(i) mengenal pasti kerentanan (*vulnerability*);
(ii) mengenal pasti ancaman (*threat*);
(iii) menilai risiko (*risk assessment*);
(iv) menentukan pengolahan risiko (*risk treatment*);
(v) memantau keberkesanan pengolahan risiko; dan
(vi) memantau ancaman yang berkaitan dengan baki risiko (*residual risk*) dan risiko yang diterima.

9. PEMATUHAN PENGURUSAN MAKLUMAT RAHSIA RASMI

9.1. Pematuhan pengurusan maklumat rahsia rasmi dalam persekitaran ICT menjadi prasyarat (prerequisite) terhadap sebarang cadangan penggunaan perkhidmatan pengkomputeran awan. Perkara-perkara yang perlu dipatuhi ialah seperti berikut;

9.1.1. **Klasifikasi Maklumat**

(a) Bagi cadangan penggunaan pengkomputeran awan, Jabatan perlu merujuk kepada tatacara pengendalian maklumat rahsia rasmi dan juga Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) bagi urusan berkaitan pewujudan, pengelasan, pengendalian, simpanan, pelepasan dan pelupusan maklumat.

(b) Pengelasan data, maklumat dan rekod rahsia rasmi hendaklah dilaksanakan terlebih dahulu dan berpandukan kepada peraturan dan arahan yang berkuat kuasa.

(c) Klasifikasi maklumat memudahkan pengurusan menentukan tahap perlindungan dan kawalan mengikut peringkat keselamatan yang bersesuaian bagi memenuhi keperluan undang-undang dan peraturan berkaitan. Antara kaedah kawalan keselamatan yang perlu dipertimbangkan adalah seperti kawalan akses pelbagai, mekanisme penyulitan, sanitasi data dan lain-lain seumpamanya. Semua kawalan tersebut hendaklah dipersetujui dan didokumenkan.

(d) Penggunaan peringkat keselamatan yang tidak tepat dalam membuat penentuan klasifikasi maklumat memberi kesan dan impak seperti di bawah:

(i) *under-classification* boleh mengakibatkan maklumat kerajaan yang diuruskan dalam perkhidmatan pengkomputeran awan tidak mempunyai kawalan keselamatan yang bersesuaian dan terdedah kepada risiko; dan

(ii) *over-classification* pula membebankan kepada pengguna yang mengendalikan maklumat kerajaan, peningkatan kos kerana kawalan yang berlebihan dan menyebabkan pemilihan perkhidmatan pengkomputeran awan dilakukan dengan tidak tepat.

9.1.2. **Bidang Kuasa**

Semua maklumat rahsia rasmi yang **disimpan dan diproses hendaklah berada di bawah kawalan dan bidang kuasa undang-undang Kerajaan Malaysia**. CSP hendaklah memastikan semua maklumat rahsia rasmi tersebut kekal dikendalikan di dalam persekitaran atau kemudahan (facility) yang diperakui oleh Kerajaan sahaja selaras dengan Arahan Keselamatan (Semakan dan Pindaan 2017), Akta 88 dan undang-undang lain berkaitan.

9.1.3. **Kawalan Pengguna**

Jabatan hendaklah memastikan supaya capaian sesuatu data yang kritikal atau maklumat rahsia rasmi dihadkan kepada pengguna tertentu sahaja (authorized user) yang boleh mengakses fail secara spesifik. Individu yang mempunyai akses kepada maklumat rahsia rasmi adalah bertanggungjawab ke atas tindakan masing-masing dan tertakluk kepada peraturan dan peruntukan keselamatan seperti yang dinyatakan di dalam Arahan Keselamatan (Semakan dan Pindaan 2017). Akauntabiliti ini hendaklah diperjelaskan kepada semua pengguna yang mempunyai akses sumber pengkomputeran awan tersebut.

9.1.4. **Khidmat Nasihat Undang-Undang**

Jabatan hendaklah mendapatkan khidmat nasihat penasihat undang-undang berhubung dengan kebolehupayaan kuasa perundangan asing diberi kebenaran akses kepada maklumat atau aplikasi Jabatan

terutamanya yang diurus oleh CSP asing. Ini adalah kerana, pihak CSP asing juga tertakluk kepada kuasa perundangan dan pentadbiran negara berkenaan.

9.1.5. **Kaedah Penentuan Residensi Data**

(a) Jabatan hendaklah mematuhi dasar berhubung kaedah pemilihan model pelaksanaan dan kawalan residensi data seperti yang diperjelaskan di bawah **LAMPIRAN 1.**

(b) Peringkat keselamatan bagi data terkawal, Terhad dan Sulit boleh berada di luar negara dengan syarat dan ketetapan seperti berikut;

(i) bagi tujuan sandaran data sahaja. Data yang mempunyai maksud rahsia rasmi hendaklah mematuhi keperluan pengurusan mekanisma kawalan rahsia rasmi;

(ii) Ketua Jabatan hendaklah menilai terlebih dahulu liabiliti atau obligasi undang-undang yang berkaitan sama ada di dalam atau di luar negara sebelum membuat sebarang keputusan yang melibatkan pemindahan data tersebut ke luar negara; dan

(iii) Jabatan hendaklah mendapatkan persetujuan dan kebenaran daripada pihak berkuasa berkaitan yang mengawal selia pelepasan data atau maklumat Kerajaan ke luar negara.

9.1.6. **Pengurusan dan Kawalan Kriptografi**

Jabatan hendaklah memastikan pengurusan dan kawalan kriptografi berada di bawah kawalan dan tanggungjawab sepenuhnya pihak Kerajaan. Bagi menjamin kedaulatan data, sebarang kekunci kriptografi yang memberi implikasi besar kepada keselamatan hendaklah menggunakan perkakasan yang dibenarkan setelah melalui penilaian keselamatan dan disimpan di premis Kerajaan dalam negara.

CSP hendaklah menyediakan infrastruktur sokongan berkaitan bagi memastikan strategi kawalan ini boleh dilaksanakan.

9.1.7. **Pengecualian Residensi Data**

Umumnya, penawaran model *public cloud* dipercayai lebih menjimatkan berbanding model pelaksanaan yang lain. Model ini membenarkan *transborder data flow* dan secara langsung residensi data boleh berada di *onshore* atau *offshore*. Daripada perspektif teknologi, ada pelbagai mekanisma kawalan bagi melindungi data tetapi data tersebut dikhuatiri mempunyai beberapa risiko tambahan terutamanya melibatkan isu perundangan. Bagi menjamin kedaulatan data dan aset strategik Kerajaan, pemilihan model ini dikecualikan bagi kategori data atau maklumat yang mempunyai implikasi keselamatan seperti di **LAMPIRAN 2**.

10. PENGURUSAN KONTRAK DAN TERMA KESELAMATAN

10.1. ***Due Diligence***

10.1.1. Sebelum sebarang keputusan untuk menggunakan perkhidmatan pengkomputeran awan dibuat, Jabatan hendaklah membuat penilaian secara terperinci berdasarkan kepada keperluan, pematuhan kepada dasar sedia ada dan kekangan undang-undang yang berkaitan.

10.1.2. Dalam keadaan tertentu, laporan *Cost Benefit Analysis* (CBA) juga diperlukan bagi membantu pihak Jabatan membuat penilaian risiko dan merancang strategi pemilihan perkhidmatan pengkomputeran awan. Ini kerana terdapat kebarangkalian berlakunya situasi *vendor lock-in* berpunca daripada isu kos. Sebagai contoh, kos bagi *data egress* tidak diketahui atau diperjelaskan di peringkat awal. Perkara ini boleh menyebabkan berlaku pertikaian kewangan dan akhirnya

persetujuan di antara pelanggan dan penyedia perkhidmatan gagal diperoleh.

10.1.3. Jabatan hendaklah memastikan supaya isi kandungan kontrak seperti *Customer Agreement*, *Service Level Agreement* (SLA) atau *Acceptable Use Policy* (AUP) difahami sebelum mendaftar untuk menggunakan sebarang perkhidmatan. Jabatan boleh mempertimbangkan CSP lain sekiranya sebarang terma di dalam kontrak tidak difahami dan meragukan.

10.2. ***Service Level Agreement*** **(SLA)**

10.2.1. Kebiasaannya SLA yang terkandung dalam kontrak menerangkan tahap perkhidmatan yang dipersetujui melalui beberapa faktor (attributes) seperti ketersediaan, prestasi atau kebolehkhidmatan (serviceability).

10.2.2. SLA hendaklah menjelaskan *threshold matrix* bersama dengan penalti kewangan sekiranya berlaku gangguan perkhidmatan atau pelanggaran kontrak.

10.3. **Hak Milik Data (Data Ownership)**

10.3.1. Spesifikasi perolehan yang disediakan oleh Jabatan hendaklah mengandungi klausa tertentu berhubung status pemilikan data (data ownership).

10.3.2. Data atau maklumat adalah hak milik eksklusif Kerajaan sepenuhnya dan tidak boleh dianggap sebagai aset kepada CSP dan Kerajaan boleh mengambil apa-apa tindakan sebagaimana yang diperlukan. Hal ini adalah bagi mengelakkan sebarang isu yang mungkin timbul sekiranya CSP telah berpindah milik, muflis atau dikenakan tindakan di bawah undang-undang.

10.3.3. Pihak CSP tidak dibenarkan menggunakan maklumat atau data Jabatan untuk tujuan komersial atau bagi maksud lain tanpa pengetahuan dan kebenaran pihak Kerajaan.

10.4. **Privasi**

Memastikan supaya data organisasi tidak disalin, diubahsuai, dipadam, diakses tanpa kebenaran Jabatan. Penyalahgunaan data organisasi melalui perkhidmatan pengkomputeran awan bukan sahaja melanggar polisi organisasi malah mungkin berhadapan dengan tindakan undang-undang yang sedang berkuat kuasa.

10.5. **Audit**

10.5.1. Kerajaan hendaklah diberikan hak untuk melaksanakan audit ke atas CSP. Jabatan hendaklah membuat semakan keperluan tersebut ada dinyatakan di dalam *Terms of Service* CSP.

10.5.2. Dalam kes yang tertentu hak audit tersebut boleh disandarkan kepada pihak ketiga yang tidak mempunyai sebarang kepentingan terhadap penyedia perkhidmatan atas persetujuan pihak Kerajaan.

10.5.3. Audit ini berfungsi sebagai satu kaedah bagi memastikan tiada sebarang kerentanan dan ketidakakuran keselamatan berlaku selain dapat memastikan aktiviti pengurusan risiko diuji secara berkala, menyeluruh dan dikemas kini sewajarnya.

10.5.4. Audit metodologi yang digunakan juga hendaklah mengambil kira semua proses kitar hayat maklumat bagi memastikan keberkesanan langkah-langkah kawalan yang diambil, mencukupi dan berada dalam keadaan baik serta berfungsi sepanjang masa.

10.6. **Pampasan (*Compensation*)**

Insiden atau pelanggaran keselamatan boleh memberi implikasi dan kerosakan yang besar (catastrophic) terhadap reputasi, imej, kewangan, keselamatan dan pertahanan. Jabatan hendaklah memastikan CSP memberi perlindungan dan membayar ganti rugi (indemnification) sekiranya insiden berpunca daripada kesalahan oleh pihak penyedia perkhidmatan (klausa *indemnification* yang terkandung di dalam kontrak kebiasaannya untuk melindungi CSP daripada dikenakan saman daripada pihak pengguna).

10.7. **Liabiliti**

Jabatan hendaklah menilai had liabiliti yang mungkin wujud akibat daripada gangguan perkhidmatan yang berlaku di luar kawalan CSP. Perkara tersebut termasuklah gangguan bekalan kuasa, pergantungan perkhidmatan oleh undang-undang, *force majeure* atau isu capaian internet dari *Internet Service Provider* (ISP).

10.8. **Hak Mencapai Elemen**

Semua spesifikasi perolehan dan kontrak komersial hendaklah mengandungi penyataan mandatori seperti yang berikut:

"*CSP hendaklah memberi hak mencapai elemen sistem yang mengandungi maklumat rasmi dan maklumat rahsia rasmi, pihak Kerajaan boleh mengambil tindakan sebagaimana yang diperlukan*".

10.9. **Pelucutan Perkhidmatan (Exit Process)**

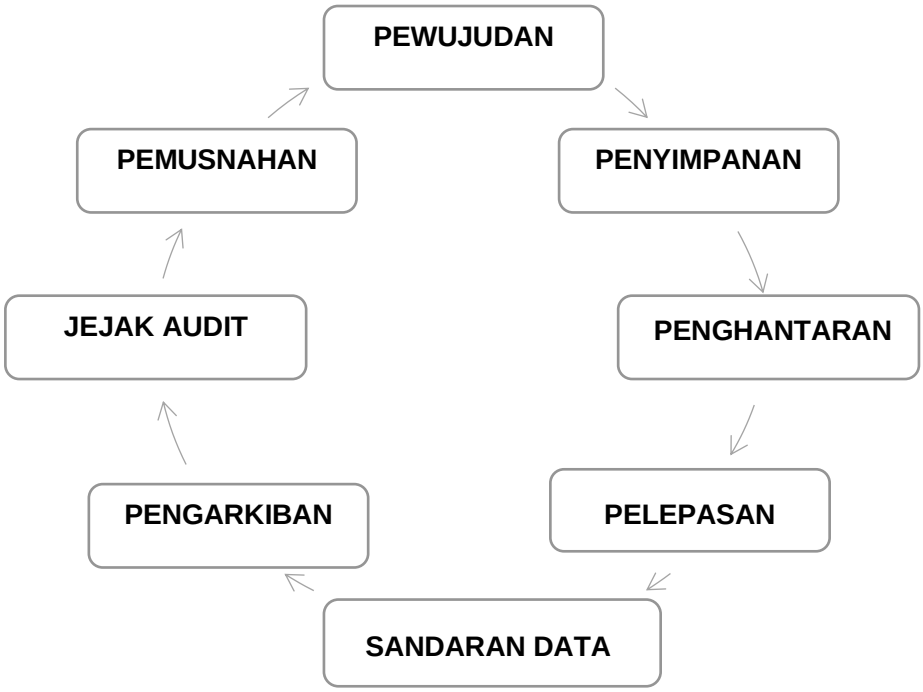
10.9.1. Klausa berhubung dengan pelucutan pentauliahan (decommissioning) atau penamatan kontrak hendaklah dinyatakan dengan jelas di dalam kontrak perkhidmatan. Ia termasuklah tanggungjawab pihak Jabatan dan CSP sekiranya kontrak

ditamatkan lebih awal seperti kegagalan CSP mematuhi SLA atau daripada sebarang faktor yang lain.

10.9.2. Jabatan hendaklah memastikan exit plan disediakan bagi memastikan proses transisi dan migrasi berjalan dengan lancar tanpa kehilangan, kerosakan atau ketirisan data. Jabatan juga mempunyai tempoh masa yang bersesuaian untuk membuat salinan data dan log berkaitan seperti log sistem, log rangkaian, log pelayan, log transaksi dan *audit trail* sehingga *exit process* dilaksanakan sepenuhnya.

11. KEPENTINGAN MELINDUNGI MAKLUMAT DALAM PERSEKITARAN ICT

11.1. Perlindungan ke atas maklumat yang dikendalikan dalam persekitaran ICT khususnya dalam pengkomputeran awan hendaklah mengambil kira setiap proses kitaran hayat maklumat tersebut seperti di Rajah 1. Ini termasuk kepada komponen peralatan, pangkalan data dan aplikasi yang ada pada sistem pengkomputeran awan.



Rajah 1 : Kitaran Hayat Maklumat

12. KAEDAH PERLINDUNGAN DATA DAN MAKLUMAT

12.1. Keselamatan data atau maklumat memerlukan teknologi dan kawalan yang spesifik bagi menguatkuasakan peraturan dan peruntukan keselamatan. Perkara-perkara yang perlu diberi perhatian adalah perlindungan migrasi data ke pengkomputeran awan, perlindungan data semasa penghantaran dan perlindungan data dalam simpanan logikal atau fizikal oleh pihak penyedia perkhidmatan.

12.2. Antara kaedah kawalan yang perlu dilaksanakan adalah seperti perkara di bawah:

12.2.1. **Enkripsi**

(a) Jabatan atau CSP hendaklah memastikan ciri-ciri keselamatan maklumat seperti kerahsiaan, kebolehsediaan dan integriti data dilindungi. Kerahsiaan dan integriti data atau maklumat boleh dilindungi melalui kaedah penyulitan (enkripsi) di semua peringkat transaksi dan aliran data.

(b) Memastikan supaya data sentiasa dienkrip dalam semua keadaan (data at rest, data in motion, data in use) sebelum disimpan di dalam pengkomputeran awan bagi meminimakan kesan insiden sekiranya perkhidmatan pengkomputeran awan tersebut dikompromi.

(c) Di antara kawalan keselamatan yang boleh diaplikasi dalam penghantaran data (data in motion) adalah seperti penggunaan saluran komunikasi selamat (HTTPS, SFTP, VPN yang menggunakan SSL atau IPSec dan TLS) di mana pengurusan kunci, algoritma dan panjang kunci (key length) memenuhi syarat-syarat keselamatan.

(d) Kaedah enkripsi ini juga hendaklah dilaksanakan ke atas penggunaan *virtualization*, *multi tenant* dan penyimpanan sandaran data khususnya dalam perkhidmatan PaaS dan SaaS.

(e) Penggunaan Produk Kriptografi Terpercaya (PKT) adalah mandatori di dalam urusan yang melibatkan maklumat rahsia rasmi selaras dengan Dasar Kriptografi Negara.

(f) Pengurusan kunci (encryption key management) hendaklah mematuhi Arahan Teknologi Maklumat.

12.2.2. **Pengasingan**

(a) Maklumat rahsia rasmi hendaklah disimpan dan diproses di dalam infrastruktur pengkomputeran awan yang khusus (dedicated) dan ditempatkan di dalam fasiliti yang diperakui oleh Kerajaan.

(b) Aliran data bagi maklumat rahsia rasmi hendaklah diasingkan secara logikal (software/virtualization-based architectures) mahupun fizikal (rangkaian, storan, pangkalan data) dalam setiap model pengkomputeran awan.

(c) Rekabentuk dan mekanisma *multi-tenancy* yang disediakan oleh CSP hendaklah dinilai oleh Jabatan terlebih dahulu bagi memastikan maklumat tidak boleh diakses oleh pengguna sah yang lain (tenant) yang menggunakan perisian dan sumber yang sama.

12.2.3. **Pengurusan Akses dan Identiti**

(a) Pengurusan akses dan identiti adalah fungsi kritikal bagi sesebuah Jabatan yang menggunakan pengkomputeran awan. Seksyen ini menerangkan maklumat berkaitan dengan pengesahan (authentication), kawalan had akses dan pengasingan tugas dan

tanggungjawab (segregation of duties) bagi setiap kakitangan yang terlibat dengan perkhidmatan pengkomputeran awan.

(b) Ciri-ciri asas pengkomputeran awan seperti akses rangkaian yang meluas (broad network access) memerlukan Jabatan mempunyai kitaran pengurusan identiti yang kukuh (robust) untuk dilaksanakan. Ini kerana, pengguna boleh membuat capaian ke atas maklumat atau sumber pengkomputeran dari pelbagai lokasi dan peralatan yang dikhuatiri boleh memberi kesan dan risiko keselamatan.

(c) Oleh itu, pengurusan identiti dan kawalan akses pengguna hendaklah dikaji dan disediakan bagi memastikan penggunaan perkhidmatan pengkomputeran awan dapat dicapai dengan selamat dan mudah oleh pengguna. Antara proses dan kawalan yang perlu dilaksanakan adalah meliputi perkara berikut:

(i) sumber pengkomputeran awan hanya boleh di akses oleh pengguna yang sah sahaja;

(ii) akses hanya akan diberikan sekiranya peranan atau fungsi pengguna yang memerlukan maklumat atau sumber tersebut;

(iii) CSP yang ada menyediakan *Role Based Access Control* (RBAC) dapat membantu Jabatan menguruskan sumber pengkomputeran dengan lebih baik seperti membuat penetapan siapa dan apakah yang mereka boleh lakukan dengan sumber tersebut;

(iv) hak akses pengguna hendaklah dikaji dengan segera atau ditarik balik apabila berlaku perubahan profil pengguna;

(v) akaun pengguna hendaklah ditamatkan sebaik sahaja pengguna diberhentikan atau tidak lagi diberi kebenaran untuk akses kepada pengkomputeran awan;

(vi) Jabatan hendaklah memastikan penggunaan kata laluan yang panjang dan selamat untuk mengesahkan perkhidmatan pengkomputeran awan;

(vii) capaian akses terhadap perkhidmatan pengkomputeran awan yang mengandungi maklumat rahsia rasmi hendaklah berdasarkan lebih daripada satu pengenalan pengguna (Multi Factor Authentication);

(viii) fungsi pengesahan pengguna hendaklah diasingkan daripada aplikasi tersebut bagi pengurusan berpusat. Ini bertujuan untuk memudahkan pengguna dan membolehkan tindak balas segera terhadap ancaman; dan

(ix) semua sistem maklumat ICT yang menggunakan pengkomputeran awan hendaklah berupaya untuk merekod dan mengesan tindakan pengguna.

12.2.4. **Perisian dan Aplikasi Keselamatan**

(a) Memastikan aplikasi keselamatan yang digunakan adalah efektif, diselenggara secara berkala (kemaskini versi, polisi dan lain-lain), dipercayai dan sah digunakan.

(b) Aplikasi atau produk keselamatan siber yang boleh digunakan termasuklah *Antivirus*, *Advanced Threat Protection* (ATP), *Next Generation Firewall* (NGFW), *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Data Leakage Protection* (DLP), *Web Application Firewall* (WAF) dan lain-lain fungsi seumpamanya.

12.2.5. **Penilaian Tahap Keselamatan**

(a) Jabatan hendaklah memastikan supaya produk keselamatan siber yang ingin digunakan mematuhi penilaian keselamatan seperti berikut:

(i) menjalani pengujian keselamatan seperti pengujian penembusan secara berkala (tahunan);

(ii) menjalani audit konfigurasi produk dan sistem secara berkala (tahunan);

(iii) mendapat pensijilan Common Criteria EAL2 yang tertakluk di bawah pengiktirafan *Common Criteria Recognition Authority* (CCRA) atau pensijilan lain yang setaraf dengannya daripada badan pensijilan yang diiktiraf Kerajaan; dan

(iv) mendapat pensijilan skema *Technology Security Assurance* (TSA) atau pensijilan lain yang setaraf dengannya daripada badan pensijilan yang diiktiraf Kerajaan.

(b) Selain itu, penilaian tahap keselamatan juga perlu dilaksanakan ke atas semua elemen pengkomputeran awan berdasarkan kepada konsep perlindungan secara mendalam (security-in-depth) meliputi komponen seperti berikut :

(i) *Web Interface*;
(ii) *Authentication/Authorisation*;
(iii) *Network Services*;
(iv) *Transport Encryption*;
(v) *Crypto System*;
(vi) *Cloud Interface*;
(vii) *Mobile Interface*;
(viii) *Security Configurability*;

(ix) *Software/Firmware*; dan

(x) *Physical Security.*

(c) Sebarang penilaian pematuhan teknikal seperti aktiviti *Security Posture Assessment* (SPA) hendaklah dijalankan oleh individu yang kompeten dan dibenarkan.

12.2.6. **Sanitasi Data**

(a) Sanitasi merujuk kepada proses untuk menjadikan capaian akses ke atas data atau maklumat yang terkandung dalam media elektronik tidak lagi dapat dilaksanakan walaupun dengan tahap usaha yang tertentu. Sanitasi data merupakan satu elemen penting yang digunakan semasa proses pelupusan maklumat di dalam sistem pengkomputeran awan. Tujuan utama pelaksanaan sanitasi data adalah bagi melupuskan maklumat secara kekal yang melibatkan beberapa proses dan kaedah tertentu digunakan seperti menulis ganti, penyingkiran, *degaussing*, pemusnahan media secara fizikal atau lain-lain kaedah bagi melindungi ketirisan maklumat.

(b) Jabatan hendaklah menentukan prosedur pelupusan maklumat dalam fasiliti pengkomputeran awan CSP dapat dilakukan mengikut kehendak keselamatan.

(c) CSP boleh mengemukakan dengan jelas kaedah sanitasi dan kawalan yang diambil sewaktu maklumat ingin dilupuskan. Dalam keadaan tertentu, pihak CSP mungkin tidak dapat menyediakan proses dan kaedah pelupusan maklumat yang bersesuaian dengan klasifikasi maklumat.

(d) Proses sanitasi data juga hendaklah dilaksanakan ke atas semua salinan sandaran data (backup, recovery centre) terutamanya selepas pelucutan pentauliahan kontrak (decommissioning).

Sanitasi juga perlu dilaksanakan apabila skala perkhidmatan seperti penggunaan ruang storan dikurangkan (scales down).

(e) Proses sanitasi data sama ada dalam media storan dan peranti elektronik hendaklah merujuk kepada Surat Pekeliling Am Bilangan 4 Tahun 2022 - Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam.

(f) *Cryptographic Erase* (CE) merupakan satu kaedah yang boleh dipertimbangkan bagi melaksanakan sanitasi data di dalam persekitaran pengkomputeran awan. CE memanfaatkan teknologi kriptografi dengan memusnahkan kunci enkripsi (encryption key) dan menyebabkan hanya teks sifer masih kekal di dalam media storan. Kaedah ini berkesan untuk menghalang *read-access* ke atas data oleh pihak yang tidak dibenarkan dan menjadikan proses pemulihan data tidak boleh dilaksanakan (infeasible).

12.2.7. **Ketirisan Data / Maklumat**

(a) Kesedaran dan pengetahuan yang tidak begitu mendalam pegawai awam dalam mengendalikan rahsia rasmi boleh menyebabkan data kritikal Kerajaan dipindahkan ke dalam pengkomputeran awan secara tidak sengaja. Kawalan ketirisan ini boleh dibuat melalui penetapan polisi dan penggunaan penyelesaian teknologi seperti sistem *Data Leakage Protection* (DLP) dan *Digital Rights Management* (DRM).

(b) Sekiranya maklumat rahsia rasmi telah dipindahkan, proses sanitasi yang sepadan dengan klasifikasi maklumat hendaklah dilakukan. Pihak CSP tidak boleh dipertanggungjawabkan dan tidak mempunyai liabiliti atas kecuaian pengguna daripada pihak pelanggan. Jabatan disarankan membuat perjanjian awal dengan

pihak CSP supaya kelonggaran diberi agar media storan yang menyimpan rahsia rasmi diberi akses untuk tujuan sanitasi.

13. KAWALAN KESELAMATAN FIZIKAL PUSAT DATA DAN INFRASTRUKTUR ICT

13.1. Di dalam perkhidmatan pengkomputeran awan, kawalan keselamatan terhadap pusat data dan infrastruktur ICT adalah di bawah tanggungjawab dan kawalan CSP.

13.2. Antara kawalan yang perlu dilaksanakan adalah seperti perkara di bawah:

13.2.1. Penilaian Keselamatan

(a) Jabatan hendaklah memastikan penilaian keselamatan secara menyeluruh dilaksanakan bagi memastikan kawalan keselamatan disediakan oleh penyedia perkhidmatan mengikut standard dan peraturan yang sedang berkuat kuasa.

(b) Penilaian adalah meliputi pemilihan lokasi, reka bentuk dan susun atur fizikal pusat data, sistem pengkabelan rangkaian, sistem penyejukan (HVAC), sistem elektrikal, sistem pengesanan dan pencegahan kebakaran, sistem pengurusan keselamatan, sistem kawalan dan pemantauan persekitaran.

(c) Kawalan keselamatan fizikal yang bersesuaian juga hendaklah diaplikasikan kepada semua tempat, bilik dan fasiliti yang menyokong perkhidmatan pengkomputeran awan tersebut.

13.2.2. Kawasan Terperingkat

Fasiliti CSP atau pusat data yang menyimpan atau menguruskan rahsia rasmi boleh membawa maksud kepada kawasan terperingkat dan perlu diberi perlindungan sepenuhnya selaras dengan

perenggan 39, Arahan Keselamatan (Semakan dan Pindaan 2017). Bagi menentukan keperluan untuk mengisytiharkan kawasan tersebut di bawah Akta Kawasan Larangan Dan Tempat Larangan 1959 [*Akta 298*] dan Akta 88, satu rujukan mestilah dibuat kepada Ketua Pengarah Keselamatan Kerajaan.

13.2.3. **Pematuhan dan Pensijilan Keselamatan**

(a) Pihak CSP adalah tertakluk kepada peraturan yang telah ditetapkan di bawah mana-mana akta berkaitan dan hendaklah melaksanakan apa jua kawalan seperti yang diperuntukkan kepadanya termasuklah memenuhi prosedur pematuhan.

(b) Pusat data yang telah mendapat pensijilan keselamatan dari badan-badan yang diiktiraf Kerajaan atau badan antarabangsa adalah digalakkan dan diutamakan.

13.2.4. **Tapisan Keselamatan**

(a) Komuniti Keselamatan

Komuniti Keselamatan yang terlibat dalam mengurus dan mengendalikan pengkomputeran awan hendaklah menjalani proses dan lulus Tapisan Keselamatan.

(b) Perakuan Akta Rahsia Rasmi 1972

Komuniti Keselamatan juga dikehendaki menandatangani Perakuan Akta Rahsia Rasmi 1972 pada LAMPIRAN “E” dan “F” seperti mana kehendak Arahan Keselamatan (Semakan dan Pindaan 2017).

13.2.5. **Validasi Keselamatan Rahsia Rasmi**

Jabatan hendaklah merujuk ke Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia bagi mendapatkan khidmat nasihat berhubung penilaian perkhidmatan pengkomputeran awan yang hendak digunakan bagi tujuan rahsia rasmi.

13.2.6. **Sokongan**

Mengenal pasti CSP yang boleh memberikan maklum balas pantas sekiranya pengguna menghadapi sebarang masalah pada sistem. Antara *platform* sokongan yang boleh digunakan adalah seperti telefon, e-mel atau laman sesawang yang mempunyai forum maklum balas seperti ruangan soalan lazim dan lain-lain.

13.2.7. **Notifikasi**

CSP hendaklah memaklumkan kepada pengguna terhadap sebarang insiden atau pelanggaran keselamatan mengikut SOP yang ditetapkan.

14. PENGURUSAN INSIDEN

14.1. Pihak Jabatan hendaklah memastikan pengurusan maklumat dalam pengkomputeran awan boleh dipantau menerusi mekanisma pemantauan keselamatan yang bersesuaian sama ada di peringkat jabatan atau secara berpusat bagi tujuan penyelarasan sebarang insiden ancaman siber yang berkemungkinan boleh berlaku ke atas infrastruktur pengkomputeran awan.

14.2. Pihak Jabatan perlu merujuk Polisi Keselamatan Siber mengenai pengurusan insiden terkini yang diwujudkan oleh Jabatan masing-masing.

14.3. Semua insiden perlu dibuat penilaian implikasi dan taksiran risiko keselamatan di peringkat Jabatan sebelum dilaporkan kepada agensi bertanggungjawab untuk tindakan selanjutnya.

15. PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

15.1. Jabatan hendaklah memastikan CSP mewujudkan atau mempunyai pelan pengurusan kesinambungan perkhidmatan (PKP) bagi menjamin fungsi dan perkhidmatan yang dipindahkan ke pengkomputeran awan dapat dipulihkan sekiranya berlaku sebarang gangguan atau kegagalan kepada infrastruktur pengkomputeran awan.

15.2. Dalam keadaan tertentu, Jabatan diberi kebenaran bagi menguji dan membuat penilaian secara *on-site* di fasiliti CSP bagi menentukan kawalan dan langkah yang akan diambil semasa dan selepas berlaku bencana.

15.3. Jabatan juga boleh membuat semakan dan pengesahan dokumen PKP sekiranya CSP mempunyai pensijilan berkaitan *Business Continuity Management* (BCM) daripada mana-mana badan bertauliah. Apabila PKP diuji satu notifikasi atau makluman rasmi kepada Jabatan hendaklah dibuat tanpa mengira sama ada ianya memenuhi SLA atau pun tidak.

16. KEBOLEHSEDIAAN DAN SANDARAN DATA

16.1. Jabatan tidak seharusnya bergantung sepenuhnya terhadap penyedia perkhidmatan apabila berlaku gangguan. Satu pelan pemulihan bencana hendaklah disediakan bagi memudahkan proses migrasi dan *failover* dilakukan dalam tempoh masa yang bersesuaian.

16.2. Kontrak hendaklah menyatakan dengan jelas obligasi CSP untuk memastikan sistem atau perkhidmatan dapat dibaik pulih (restore) dalam tempoh yang ditetapkan apabila berlaku kegagalan pada sumber pengkomputeran awan. Data validasi juga boleh dilakukan secara automatik bagi memeriksa integriti data pada bila-bila masa yang diperlukan. Selain itu,

CSP mempunyai sumber dan polisi berhubung dengan proses sandaran data yang mudah diuruskan secara atas talian.

16.3. Dalam konteks yang lain, pihak Jabatan hendaklah mempertimbangkan untuk melaksanakan proses sandaran data sama ada di infrastruktur penyedia perkhidmatan yang berbeza atau di premis sendiri atau di mana-mana pusat repositori data yang disahkan atau di bawah milikan pihak Kerajaan.

17. KESIMPULAN

17.1. Garis panduan ini disediakan sebagai panduan dan rujukan kepada Jabatan mengenai pengurusan perkara rasmi dan rahsia rasmi dan kepentingan melaksanakan langkah-langkah kawalan keselamatan perlindungan dalam persekitaran pengkomputeran awan bagi memastikan keselamatan aset dan maklumat Kerajaan terjamin sepanjang masa.

18. RUJUKAN

1. Akta Rahsia Rasmi 1972 [*Akta 88*]
2. Akta Arkib Negara 2003 [*Akta 629*]
3. Akta Tandatangan Digital 1997 [*Akta 562*]
4. Akta Perlindungan Data Peribadi 2010 [*Akta 709*]
5. Akta Kawasan Larangan Tempat Larangan 1959 [*Akta 298*]
6. Akta Keterangan 1950 [*Akta 56*]
7. Arahan Keselamatan (Semakan dan Pindaan 2017)
8. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara
9. Arahan Teknologi Maklumat 2007
10. Dasar Kriptografi Negara 2013
11. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)
12. Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).

13. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
14. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam.
15. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)
16. Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam
17. Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam
18. Arahan-arahan lain yang sedang berkuat kuasa
19. ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements
20. ISO/IEC 27017:2015 Information Technology – Security Techniques – Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services
21. ISO/IEC 22301: 2010 Security and Resilience – Business continuity management system – Requirements
22. NIST Special Publication 800-145 - The NIST Definition of Cloud Computing
23. NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing
24. NIST Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems
25. NIST Cloud Computing Reference Architecture (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292
26. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing
27. OWASP Top 10 Application Vulnerabilities

LAMPIRAN 1

MATRIK KLASIFIKASI MAKLUMAT DALAM PELAKSANAAN PENGKOMPUTERAN AWAN DALAM PERKHIDMATAN AWAM

Klasifikasi Maklumat	Peringkat Keselamatan	Tradisional (Pusat Data Jabatan)	MODEL CLOUD YANG DIBENARKAN			RESIDENSI DATA			
			Public	Private	Hybrid	*Onshore* (Dalam Negara) Bagi Fasiliti / Infrastruktur Utama			*Offshore* (Luar Negara) Bagi Tujuan Sandaran Data
						On-Premise (Premis Kerajaan)		Off-Premise	Premis CSP
						CSP Tempatan (termasuk MyGovCloud@PDSA)	CSP Asing (dibangunkan untuk Kerajaan	CSP Tempatan / CSP Asing	
RASMI	Data Terbuka	/	/	/	/	/	/	/	/
	Data Terkawal (Kewangan, Rekod Perubatan, Data Peribadi atau PII)	/	/	/	/	/	/	/	/**
RAHSIA RASMI	**TERHAD**	/	/	/	/	/	/	/*	/**
	SULIT	/	/	/	/	/	/	/*	/**
	RAHSIA	Isolate	x	X	x	x	x	x	x
	RAHSIA BESAR	Isolate	x	X	x	x	x	x	x

** maklumat luar Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] sahaja*

*** sila rujuk kepada perenggan 9.1.5 (b) Garis Panduan*

139. Penggunaan pengkomputeran awan (cloud computing) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali **kecuali pengkomputeran awan yang dibangunkan dan dibenarkan** oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa

LAMPIRAN 2

SENARAI DATA ATAU DOKUMEN YANG TIDAK BOLEH DILEPASKAN ATAU DISIMPAN DI LUAR NEGARA

1. Kertas-kertas keputusan kabinet dan jawatankuasa-jawatankuasa kabinet
2. Kertas-kertas keputusan Majlis Mesyuarat Kerajaan Negeri (MMKN) dan jawatankuasa-jawatankuasa MMKN
3. Keselamatan Negara
4. Pertahanan Negara
5. Perhubungan Antarabangsa
6. Kertas-kertas siasatan dan perisikan agensi penguatkuasa
7. Hal-hal kerahsiaan di dalam perundangan
8. Keistimewaan profesional perundangan
9. Bahan-bahan Sulit Peperiksaan Awam
10. Dokumen-dokumen belanjawan negara
11. Maklumat perdagangan dan pelaburan yang rahsia lagi berharga
12. Daftar Pemilih
13. Data-data bancian
14. Maklumat operasi agensi keselamatan
15. Data peribadi pembesar negara
16. Dokumen Geospatial Terperingkat
17. Data pemberi maklumat