KEMENTERIAN SUMBER MANUSIA

TVET MALAYSIA

POLISI PERKONGSIAN DATA TVET

KEMENTERIAN SUMBER MANUSIA

TVET MALAYSIA

POLISI PERKONGSIAN DATA TVET

Cetakan Pertama Mac 2025

Diterbitkan oleh:
Jabatan Pembangunan Kemahiran

Rekabentuk oleh:
Visual Print Sdn Bhd.
No. 47, 47-1, Jalan Damai Raya 1,
Alam Damai, Cheras
56000 Kuala Lumpur

Penghargaan:
Jabatan Digital Negara, Kementerian Digital
Bahagian Dasar, Kementerian Sumber Manusia (KESUMA)
Jabatan Tenaga Manusia, Kementerian Sumber Manusia (KESUMA)
Kementerian Belia dan Sukan (KBS)
Kementerian Kemajuan Desa dan Wilayah (KKDW)
Kementerian Pendidikan Tinggi (KPT)
Kementerian Pendidikan Malaysia (KPM)
Kementerian Perladangan dan Komoditi (KPK)
Kementerian Pertanian dan Keterjaminan Makanan (KPKM)
Kementerian Kerja Raya (KKR)
Kementerian Pelancongan, Seni dan Budaya (MOTAC)
Kementerian Dalam Negeri (KDN)
Kementerian Pertahanan (MOD)
Kementerian Kerja Raya (KKR)
Kementerian Pembangunan Wanita, Keluarga dan Masyarakat (KPWKM)

ISI KANDUNGAN

SENARAI LAMPIRAN

Lampiran A : IDD bagi integrasi melalui MyGDX
Lampiran B : Templat IDD API

AKRONIM

API	Application Programming Interface
CGSO	Chief Government Security Officer
DRSA	Data Raya Sektor Awam
G2B	Government-to-Businesses
G2C	Government-to-Citizen
G2E	Government-to-Employee
G2G	Government-to-Government
GLC	Government Link Company
GIC	Government Investment Company
HLC	High Level Committee
HRDCorp	Human Resource Development Corporation
ICT	Information and Communication Technology
IDD	Interface Description Documentation
JDN	Jabatan Digital Negara
JPDTVET	Jawatankuasa Pemandu Data TVET
JTDTVET	Jawatankuasa Teknikal Data TVET
JPA	Jabatan Perkhidmatan Awam
JPK	Jabatan Pembangunan Kemahiran
MoU	Memorandum of Understanding
MTVET	Majlis TVET Negara
MyGDX	Malaysian Government Central Data Exchange
MySPIKE	Sistem Pengurusan Integrasi Kemahiran Malaysia
NoU	Note of Understanding
NGO	Non Governmental Organization
KESUMA	Kementerian Sumber Manusia
KSN	Ketua Setiausaha Negara
KSMM	Kerangka Strategik Malaysia Madani
KSU	Ketua Setiausaha
KKTD	Kumpulan Kerja Teknikal Data
KKTS	Kumpulan Kerja Teknikal Sistem
KWSP	Kumpulan Wang Simpanan Pekerja
PERKESO	Pertubuhan Keselamatan Sosial
PKPA	Pekeliling Kemajuan Pentadbiran Awam
PPDA	Pasukan Pentadbir Data Agensi
PUU	Penasihat Undang-Undang
TiPS	TVET Instructor eProfiling System
TPM	Timbalan Perdana Menteri
TVET	Technical and Vocational Education and Training
UP_TVET	Unit Pengambilan TVET

TAKRIFAN

Bagi maksud pemakaian garis panduan ini:

1. **Agensi Sektor Awam** merujuk kementerian atau jabatan kerajaan di bawah Perkhidmatan Awam Persekutuan, Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun (Persekutan dan Negeri) dan Pihak Berkuasa Tempatan.
2. **Agensi Sektor Swasta** merujuk syarikat yang ditubuhkan di bawah Akta Syarikat 1965 (termasuk syarikat kerajaan) dan organisasi swasta tempatan yang sah.
3. **Data** merujuk kepada fakta, statistik, representasi maklumat atau konsep yang disediakan dalam bentuk elektronik dan boleh disampaikan, dianalisis atau diproses.
4. **Data berkelompok** merujuk kepada data yang diekstrak melalui sistem atau secara manual yang dikumpul dan disalurkan kepada pemohon melalui sistem atau secara manual dalam bentuk berkelompok.
5. **Data peribadi** merujuk kepada data peribadi yang mengandungi maklumat peribadi individu berbentuk sulit yang dilindungi di bawah Akta Perlindungan Data Peribadi 2010 [Akta 709] seperti nama, nombor kad pengenalan, alamat kediaman, nombor telefon, Purata Nilai Gred Kumulatif, maklumat kesihatan dan maklumat fizikal individu. Data ini boleh disimpan secara manual atau elektronik.
6. **Data Rahsia Rasmi** merujuk kepada data rahsia rasmi dari Arahan Keselamatan Pindaan 2017.
7. **Data Rasmi** merujuk kepada data selain data rahsia rasmi dari Arahan Keselamatan Pindaan 2017.
8. **Data Raya TVET** merujuk kepada himpunan data TVET dalam pangkalan Data Raya TVET.
9. **Data Terbitan** merujuk kepada data baharu yang terhasil daripada aktiviti pemprosesan dan analisis data.
10. **Data Terbuka** merujuk kepada data yang boleh digunakan secara bebas, boleh dikongsi dan digunakan semula oleh rakyat dan entiti TVET untuk pelbagai tujuan.
11. **Data Terhad** adalah maklumat yang dihadkan aksesnya kepada kumpulan tertentu tetapi mungkin tidak semestinya dilindungi oleh undang-undang sepertimana data terperingkat. Data terhad mungkin mengandungi maklumat dalaman yang hanya boleh diakses oleh pihak-pihak tertentu dalam sesebuah organisasi.
12. **Data Terperingkat** adalah data sulit dan terhad.
13. **Data Tunggal** merujuk kepada data yang diekstrak melalui sistem atau secara manual yang dikumpul dan disalurkan kepada pemohon dalam satu set rekod atau boleh dipanggil sebagai data individu.
14. **Data TVET** merujuk kepada dan tidak terhad kepada data entiti TVET, pemohon, tenaga pengajar, pelajar dan sijil.
15. **Entiti TVET** merujuk kepada Agensi Sektor Awam dan Agensi Sektor Swasta yang terlibat dalam pelaksanaan TVET.
16. **G2B** merujuk kepada *Government-to-Businesses* yang dirujuk sebagai perkongsian data antara Agensi Sektor Awam dengan Komuniti Perniagaan. Komuniti perniagaan adalah termasuk tetapi tidak terhad kepada *Government Investment Company* (GIC), *Government Link Company* (GLC), majikan, syarikat swasta, Institusi Pengajian Swasta, Institusi Pendidikan Swasta, Institusi Latihan Kemahiran Swasta dan *Non Governmental Organization* (NGO).
17. **G2C** merujuk kepada *Government-to-Citizen* yang dirujuk sebagai perkongsian data antara Agensi Sektor Awam dengan rakyat. Rakyat dalam dasar ini dirujuk sebagai warganegara dan pemastautin tetap.
18. **G2E** merujuk kepada *Government-to-Employee* yang dirujuk sebagai perkongsian

data antara Agensi Sektor Awam dengan penjawat awam. Contoh data yang dikongsi: Data kehadiran, penggajian dan kenaikan pangkat.

19. **G2G** merujuk kepada *Government-to-Government* yang dirujuk sebagai perkongsian data antara Agensi Sektor Awam dengan Agensi Sektor Awam yang lain.
20. **Institusi TVET** merujuk kepada Penyedia Latihan TVET yang melaksanakan program TVET.
21. **Jawatankuasa Pemandu Data TVET (JPDTVET)** merujuk kepada jawatankuasa yang menentukan hala tuju dan strategi dasar perkongsian data TVET, memantau status pelaksanaan secara menyeluruh serta memberikan khidmat nasihat berhubung dasar dan isu-isu semasa berkaitan perkongsian data TVET.
22. **Jawatankuasa Teknikal Data TVET (JTDTVET)** merujuk kepada jawatankuasa yang bertanggungjawab dalam pemantauan pematuhan dasar perkongsian data TVET dan menyelaras program berpacukan data.
23. **Kumpulan Kerja Teknikal (KKT)** terdiri daripada Kumpulan Kerja Teknikal Data (KKTD) dan Kumpulan Kerja Teknikal Sistem (KKTS) yang merujuk kepada pasukan yang bertanggungjawab dalam membangunkan sistem Data Raya TVET termasuk menyediakan platform, analisis dan rekabentuk, penyediaan garis panduan dan dasar juga melibatkan perkara-perkara teknikal.
24. **Pasukan Pentadbir Data Agensi (PPDA)** merujuk pasukan kerja di peringkat agensi awam dan swasta yang bertanggungjawab terhadap sebarang urusan data yang ditadbir secara dalaman di agensi masing-masing.
25. **Pelajar** merujuk kepada murid, pelatih dan peserta kursus jangka pendek juga jangka panjang yang menerima latihan kemahiran atau pembelajaran di organisasi Penyedia Latihan TVET.
26. **Pembekal data** merujuk kepada Agensi Sektor Awam dan Agensi Sektor Swasta yang bertanggungjawab membekalkan data kepada pengguna secara sah dan selamat.
27. **Pemilik data** merujuk kepada Agensi Sektor Awam dan Agensi Sektor Swasta yang bertanggungjawab terhadap kualiti, integriti dan memberikan kebenaran akses kepada capaian data. Pemilik data adalah pihak yang memberikan persetujuan dan kelulusan bagi perkongsian data TVET.
28. **Pengguna data** merujuk agensi atau pihak yang memohon dan menggunakan data yang dibekalkan secara bertanggungjawab mengikut kelulusan dan terma persetujuan daripada pembekal data atau pemilik data.
29. **Pengintegrasian data** merupakan proses menyatukan data dari pelbagai sumber ke dalam satu sistem yang bertujuan untuk menghasilkan maklumat yang bermakna dan berkesan. Ia melibatkan penggunaan teknologi seperti API dan memastikan keselamatan serta integriti data, memudahkan pembuatan keputusan dan meningkatkan kecekapan pengurusan data.
30. **Pengawal data** merujuk kepada pegawai di Agensi Sektor Awam dan Agensi Sektor Swasta yang bertanggungjawab untuk menyediakan data bagi tujuan perkongsian data, mengemaskini serta menjaga keselamatan dan akauntabiliti data.
31. **Perkongsian data** merujuk kepada Agensi Sektor Awam dan Agensi Sektor Swasta yang berkongsi data secara selamat antara agensi sektor awam, swasta, penyelidik dan lain-lain bagi tujuan mengoptimumkan potensi data.
32. **Pengurusan data** merujuk kepada praktis mengumpul, menyimpan, memproses dan menggunakan data secara selamat, cekap dan berkesan.
33. **Platform perkongsian data** merujuk infrastruktur pemboleh daya perkongsian data yang disediakan oleh Sektor Awam bagi kemudahan perkongsian data merentas agensi.
34. **Rahsia Rasmi** merujuk apa-apa suratan yang dinyatakan di dalam Jadual kepada Akta Rahsia Rasmi (Akta 88) dan apa-apa

maklumat dan bahan yang berhubungan dengannya dan termasuk apa-apa dokumen 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 Akta 88.

35. **Tadbir urus** adalah proses mengawal, mengurus, dan menyelaras perkongsian data di antara pelbagai entiti TVET dengan memastikan kepatuhan terhadap piawaian, peraturan, dan undang-undang yang ditetapkan. Tadbir urus ini memastikan data dikongsi secara selamat, berintegriti, dan berkesan untuk menyokong keputusan yang lebih baik dan penyampaian perkhidmatan yang lebih efisien.
36. **UP_TVET** merujuk kepada Portal Unit Pengambilan TVET berpusat yang dibangunkan secara dalam talian untuk menyelaraskan proses permohonan kemasukan pelajar ke program TVET yang ditawarkan oleh Institusi TVET di Malaysia.

BAB 1:
PENGENALAN

1.0 PENGENALAN

1.1 Polisi ini merupakan dokumen yang menggariskan panduan kepada mana-mana agensi dalam sektor awam dan swasta bagi tatacara perkongsian data Pendidikan dan Latihan Teknikal dan Vokasional (TVET) untuk memastikan keberkesanan kecekapan pelaksanaan perkongsian data yang komprehensif dan berkesan.

1.2 Polisi ini mengandungi pernyataan prinsip yang jelas untuk membantu pembuat keputusan yang rasional dan boleh dilaksanakan sebagai asas kepada pembentukan prosedur atau protokol yang lebih terperinci. Polisi ini mesti dipatuhi dan diterima pakai oleh entiti di bawah ekosistem TVET bagi melaksanakan pengintegrasian data TVET secara menyeluruh. Tujuan dokumen ini adalah untuk menjelaskan keperluan tadbir urus, modal insan dan teknologi bagi pengintegrasian yang bertujuan membuat keputusan dan melicinkan urusan perancangan, pengurusan dan pemantauan entiti TVET.

1.3 Pengurusan TVET di Malaysia adalah merentasi pelbagai entiti TVET. Sehubungan itu, tadbir urus data TVET diperlukan bagi tujuan penyelarasan secara bersepadu melalui satu platform perkongsian data yang mapan, mampan dan selamat serta pembudayaan perkongsian data yang berterusan.

1.4 Polisi ini dipantau pelaksanaannya oleh Jabatan Pembangunan Kemahiran (JPK) di bawah Kementerian Sumber Manusia (KESUMA) untuk memandu usaha mengintegrasikan data antara jabatan, bahagian, agensi, dan institusi di bawah kelolaan entiti TVET bagi keputusan yang lebih tepat. Polisi ini merupakan panduan "living document", yang memastikan data sebagai aset diurus secara sistematik dan digunakan dengan betul semasa proses pengintegrasian data dalam ekosistem Data Raya TVET.

1.1 Tujuan

1.1.1 Polisi ini dibangunkan selaras dengan Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 2 Tahun 2021: Dasar Perkongsian Data Sektor Awam oleh Jabatan Digital Negara (JDN) bagi mengukuhkan amalan perkongsian data dan menggalakkan pembudayaan perkongsian data yang berterusan dalam kalangan sektor awam dan swasta.

1.1.2 Polisi ini juga mengandungi prosedur perkongsian data TVET yang holistik yang akan dijadikan rujukan oleh semua entiti TVET dan pihak yang berkepentingan. Dengan adanya penyepaduan perkongsian data ini membolehkan pengurusan data TVET boleh dilaksanakan secara efisien dan berstruktur.

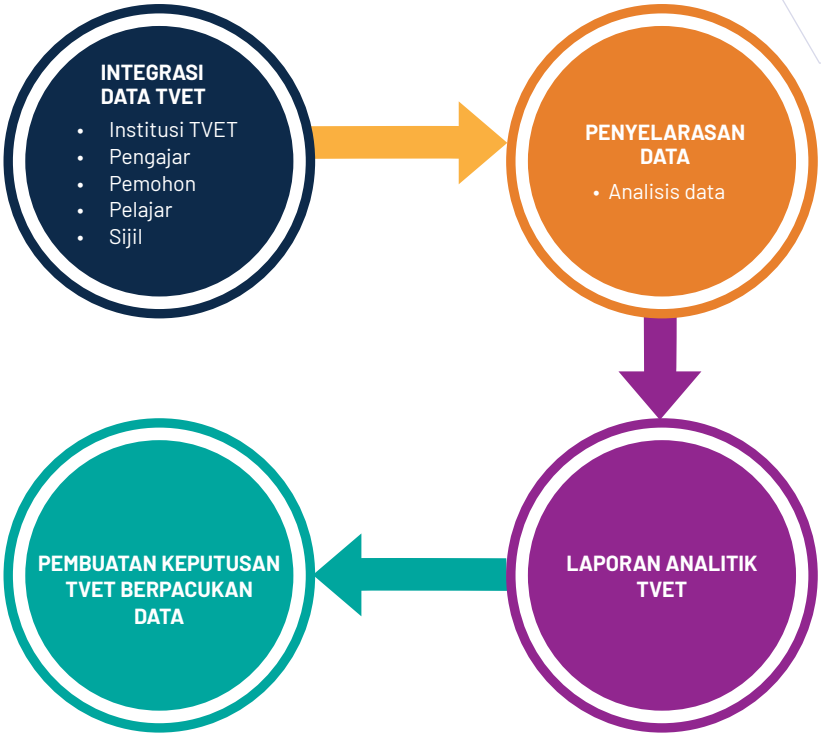
1.2 Rasional

1.2.1 Rancangan Malaysia Ke-12 (RMKe-12) melalui Strategi B5 bagi menangani pertindihan tadbir urus TVET mencadangkan untuk mewujudkan satu pangkalan data bagi menyelaras dan mengintegrasi semua data berkaitan seperti laluan TVET, ketersediaan pekerjaan dan kerjaya serta pemadanan pekerjaan.

1.2.2 Selaras dengan RMKe-12 juga, Mesyuarat Majlis TVET Negara (MTVET) Bilangan 2 Tahun 2023 yang dipengerusikan oleh Timbalan Perdana Menteri telah bersetuju supaya sistem MySPIKE yang dibangunkan oleh JPK, KESUMA dinaik taraf menjadi pangkalan Data Raya TVET dan diguna pakai oleh semua Kementerian berkaitan TVET bagi tujuan pemusatan data, penyelarasan dan perkongsian data.

1.2.3 Pembangunan Data Raya TVET ini merupakan salah satu inisiatif penambahbaikan dalam ekosistem TVET melalui penyelarasan tadbir urus data yang berstruktur, perkongsian data secara berpusat, pengintegrasian dan analitis data yang efisien dalam penawaran program TVET serta padanan pekerjaan dalam TVET yang diharap dapat meningkatkan penyampaian perkhidmatan TVET berpacukan analitis data. Ianya selaras dengan hasrat Kerajaan untuk mengelakkan pertindihan tadbir urus dalam kalangan Kementerian pelaksana TVET.

1.2.4 Pangkalan Data Raya TVET tidak terhad kepada lima (5) komponen utama data TVET iaitu maklumat entiti TVET, tenaga pengajar, permohonan, pendaftaran pelajar dan persijilan. Pengintegrasian data TVET juga tidak terhad kepada integrasi perkongsian maklumat antara entiti TVET, integrasi persijilan, integrasi carian dan padanan pekerjaan juga integrasi analisis data. Pangkalan Data Raya TVET ini berupaya untuk menyimpan dan analisis rekod data TVET secara berpusat juga membolehkan lepasan graduan TVET mencari pekerjaan melalui satu portal yang bersepadu. Proses Data Raya TVET adalah seperti **Rajah 1**.



Rajah 1 : Proses Data Raya TVET

1.3 Objektif

Objektif perkongsian data TVET adalah seperti berikut:

i. Menjadi asas dan panduan untuk perkongsian data antara entiti TVET bagi memastikan hala tuju pemusatan data dapat direalisasikan;
ii. Meningkatkan kecekapan pengurusan data merentasi entiti TVET bagi mengurangkan pertindihan dan dapat mengurangkan kos pembangunan aplikasi yang mempunyai fungsi atau skop yang sama;
iii. Meningkatkan kesepaduan perkongsian data TVET yang selamat, cekap dan berkesan dari pelbagai agensi sektor awam dan sektor swasta; dan
iv. Melonjakkan inovasi berpacukan data TVET bagi memantapkan pelaksanaan penyampaian perkhidmatan ke arah merealisasikan perkhidmatan digital entiti TVET yang bersepadu, inklusif, terangkum dan selamat.

1.4 Skop

1.4.1 Skop pelaksanaan perkongsian data ini berasaskan kepada PKPA Bilangan 2 Tahun 2021, Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional, Kementerian Digital 2022. Perkongsian data TVET ini adalah di antara entiti TVET yang telah mendapat persetujuan bersama bagi memastikan perkongsian data adalah selamat dan mematuhi tatacara yang ditetapkan di dalam Akta Rahsia Rasmi 1972 (Akta 88) dan Arahan Keselamatan (Semakan dan Pindaan 2017).

1.4.2 Perkongsian data TVET dapat direalisasikan tidak terhad kepada rekod data pendaftaran pelajar, rekod data penyedia latihan dan program yang ditawarkan, rekod data profil pengajar, rekod data persijilan, rekod data pekerjaan dan data analisis. Ringkasan perkongsian kategori data adalah seperti Jadual 1. Model Rangka Kerja Perkongsian Data TVET adalah seperti Rajah 2 dan perincian adalah seperti dalam Jadual 2.

Jadual 1: Kategori dan Deskripsi Perkongsian Data

Kategori	Deskripsi
Institusi TVET	Data institusi TVET adalah tidak terhad kepada rekod penyedia latihan, program, akreditasi, kajian pengesanan graduan, nama program.
Pelajar	Data pendaftaran pelajar tetapi tidak terhad kepada rekod pendaftaran, kumpulan, pengambilan dan penempatan pelajar, pengesanan graduan.
Pemohon	Data permohonan pelajar.
Sijil	Data persijilan pelajar adalah tidak terhad kepada rekod maklumat persijilan, persijilan professional.
Pengajar	Data profil pengajar adalah tidak terhad kepada rekod profil pengajar, kelayakan, kompetensi, penempatan

Perincian Interface Description Documentation (IDD) bagi integrasi melalui MyGDX adalah seperti di Lampiran A dan pembangunan API seperti di Lampiran B.

1.5 Prinsip Perkongsian Data TVET

Perkongsian data TVET adalah memenuhi prinsip-prinsip seperti PKPA Bilangan 1 Tahun 2021 demi kepentingan dan manfaat kepada Data Raya TVET negara. Ianya dapat meningkatkan kecekapan, menambah nilai dan memberi autonomi membuat keputusan kepada pentadbir Data Raya TVET.

i. **Perkongsian data atas keperluan dan mendapat persetujuan**
Prinsip ini menetapkan bahawa data hanya boleh dikongsi sekiranya terdapat keperluan dan persetujuan secara konsensus antara entiti TVET. Agensi yang memerlukan data hendaklah merujuk dan mendapat kelulusan daripada Jawatankuasa Teknikal Data TVET (JKTVET) terlebih dahulu dengan mematuhi prosedur dan syarat yang ditetapkan.

ii. **Perkongsian data secara selamat**
Prinsip ini menjelaskan bahawa data perlu dilindungi daripada dicerobohi, disalah guna atau dicapai secara tidak sah bagi menjamin keselamatannya di sepanjang kitaran hayat data. Data TVET sentiasa dilindungi daripada sebarang ancaman dan pengendalian data rahsia rasmi adalah tertakluk kepada Arahan Keselamatan (Semakan dan Pindaan 2017).

iii. **Perkongsian data menambah nilai kepada entiti TVET, rakyat dan negara**
Prinsip ini menetapkan bahawa data TVET perlu dimanfaatkan untuk mencipta nilai baharu dan memaksimumkan nilai data. Data yang disimpan dan dikendalikan oleh entiti TVET boleh dimanfaatkan dengan lebih cekap bagi meningkatkan penyampaian perkhidmatan yang berkesan kepada rakyat untuk meningkatkan taraf hidup rakyat dan apa-apa kegunaan lain yang memberikan manfaat kepada entiti TVET, rakyat dan negara.

1.6 Klasifikasi Data

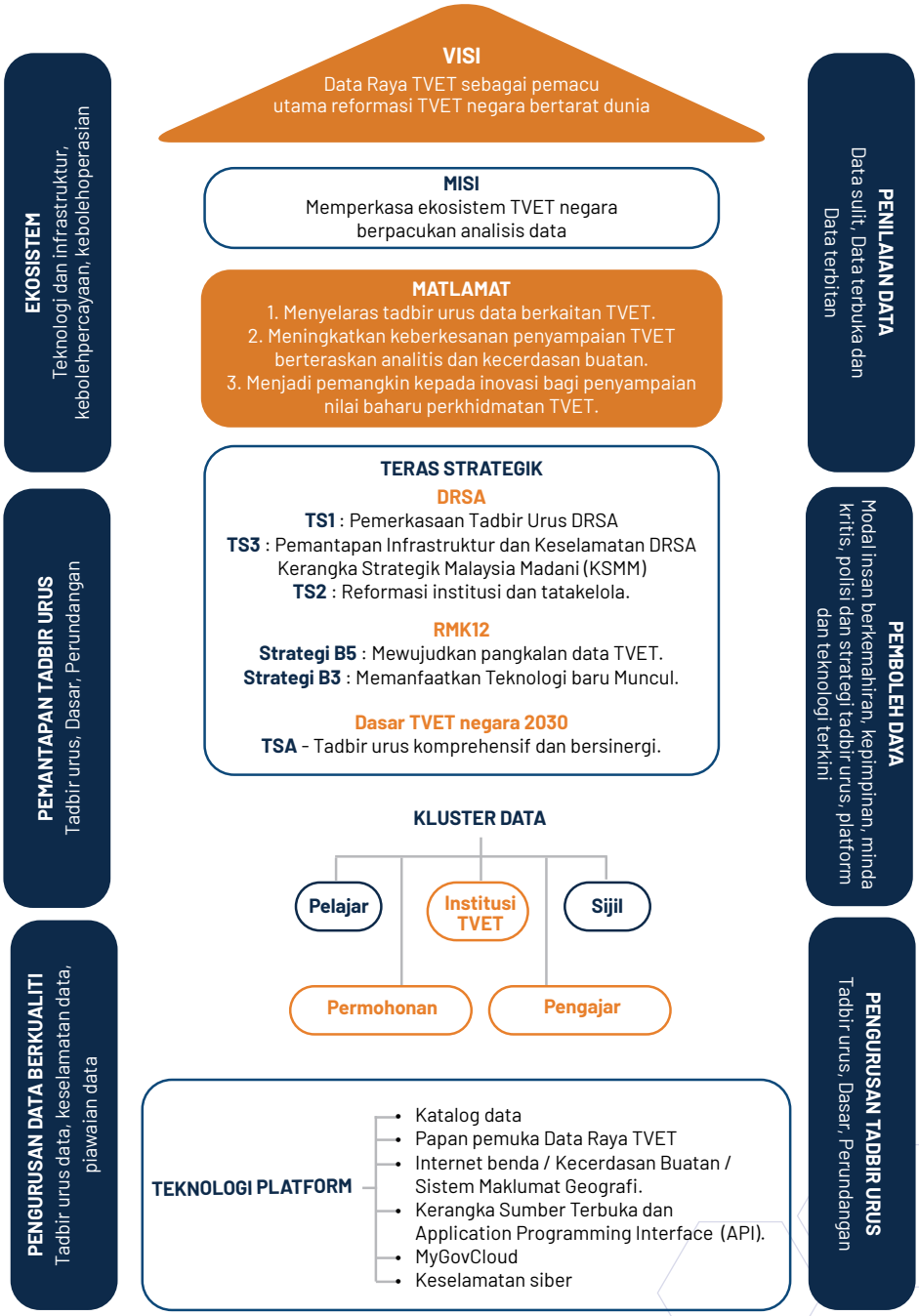
Data dikategorikan kepada data rahsia rasmi dan data rasmi. Data rahsia rasmi diklasifikasikan kepada terhad, sulit, rahsia dan rahsia besar sebagaimana yang didefinisikan di dalam Akta Rahsia Rasmi 1972 (Akta 88) dan Arahan Keselamatan (Semakan dan Pindaan 2017). Entiti TVET hendaklah mengklasifikasikan data sebelum melaksanakan perkongsian data TVET.

1.7 Manfaat Perkongsian Data TVET

Perkongsian data TVET memberi manfaat tidak terhad kepada entiti TVET seperti berikut:

i. Memperkasakan Dasar TVET Negara.
ii. Meningkatkan sistem penyampaian dan tadbir urus TVET.
iii. Meningkatkan jalinan kerjasama strategik entiti TVET.
iv. Meningkatkan kecekapan pentadbiran melalui perkongsian data TVET yang bersepadu.
v. Mengoptimumkan sumber tenaga bagi memastikan kelancaran perkongsian data secara efisien.
vi. Meningkatkan prestasi dan produktiviti.
vii. Mencegah penipuan, pembaziran, manipulasi dan penyalahgunaan data juga fasiliti secara terkawal.
viii. Pemadanan pekerjaan mengikut kelayakan yang bersesuaian dengan penggajian atau persijilan bagi pemohon dan majikan.
ix. Meningkatkan inovasi dan penyelidikan.

MODEL RANGKA KERJA PERKONGSIAN DATA RAYA TVET



Rajah 2 : Rangka kerja Data Raya TVET

Jadual 2: Perincian Rangka Kerja Data Raya TVET

Bil	Perkara	Huraian
i	**Visi**	Data Raya TVET sebagai pemacu utama reformasi TVET negara.
	Huraian	Bagi meningkatkan daya saing negara seiring negara maju, TVET adalah sektor kritikal untuk memacu pembangunan ekonomi Malaysia dan telah diketengahkan dalam Rancangan Malaysia Ke-12. Untuk menjayakan agenda reformasi TVET di Malaysia, penggubal dasar memerlukan data yang boleh dipercayai, lengkap dan bersih yang menjadi sumber dalam penggubalan dasar yang efektif seterusnya membolehkan pendekatan yang lebih padu dalam menghadapi cabaran. Data Raya TVET berfungsi sebagai repositori berpusat dan bersepadu yang menggabungkan semua data TVET bagi menambahbaik tadbir urus TVET.
ii	**Misi**	Memperkasa ekosistem TVET negara berpacukan analitik data.
	Huraian	Data Raya TVET membantu penggubal dasar untuk membuat sebarang keputusan berdasarkan analitik data.
iii	**Matlamat**	**Matlamat 1:** Menyelaras tadbir urus data berkaitan TVET. Huraian: Penyelarasan tadbir urus antara entiti TVET berkaitan perkongsian data TVET. **Matlamat 2:** Meningkatkan keberkesanan penyampaian TVET berteraskan analitik dan kecerdasan buatan. **Huraian:** Data TVET dapat disampaikan dengan berkesan melalui analitik dan kecerdasan buatan bagi membolehkan sesuatu keputusan dalam penggubalan dasar dapat direalisasikan. **Matlamat 3:** Menjadi pemangkin kepada inovasi bagi penyampaian nilai baharu perkhidmatan TVET. **Huraian:** Daripada analitik data yang dilaksanakan dapat mencetuskan inovasi dalam pembangunan dan penawaran kursus TVET.
iv	**Teras Strategik**	Rangka DRSA TS1: Pemerkasaan Tadbir Urus DRSA TS3: Pemantapan Infrastruktur dan Keselamatan DRSA Kerangka Strategik Malaysia Madani (KSMM) TS2: Reformasi institusi dan tatakelola RMKe-12 Strategi B5: Mewujudkan pangkalan data TVET Strategi B3: Memanfaatkan Teknologi Baru Muncul Dasar TVET Negara 2030 TSA – Tadbir urus komprehensif dan bersinergi

Bil	Perkara	Huraian
v	**Kluster Data**	Pelajar; Institusi TVET; Sijil; Permohonan; Pengajar
vi	**Pengelasan Data**	Data Sulit; Data Terbuka; Data Terbitan
vii	**Ekosistem perkongsian data selamat**	Teknologi dan infrastruktur, kebolehpercayaan, kebolehoperasian data
viii	**Pengurusan data berkualiti**	Tadbir urus data, Keselamatan data, Piawaian data
x	**Pemantapan tadbir urus perkongsian data**	Tadbir urus yang mantap adalah melalui pengurusan tadbir urus, dasar dan perundangan yang relevan dan produktif.
xi	**Pengukuhan kompetensi**	Pengukuhan kompetensi melalui latihan dan pembudayaan yang berkesan.
xii	**Pemboleh daya polisi data TVET**	• Modal insan berkemahiran • Kepimpinan • Minda kritis • Polisi dan strategi tadbir urus yang berkaitan • Platform dan teknologi terkini dan relevan • Peruntukan
xiii	**Prinsip Panduan**	• Dasar Perkongsian Data Sektor Awam • Perkomputeran Berpacukan Data • Dasar Pengkomputeran Awan Sektor Awam
xiv	**Teknologi Platform**	• Katalog Data • Papan pemuka Data Raya TVET • Internet Benda/ Kecerdasan Buatan/ Sistem Maklumat • Geografi • Kerangka Sumber Terbuka dan Application Programming Interface (API) • MyGovCloud • Keselamatan siber

BAB 2 :
TADBIR URUS PERKONGSIAN DATA TVET

2.0 TADBIR URUS PERKONGSIAN DATA TVET

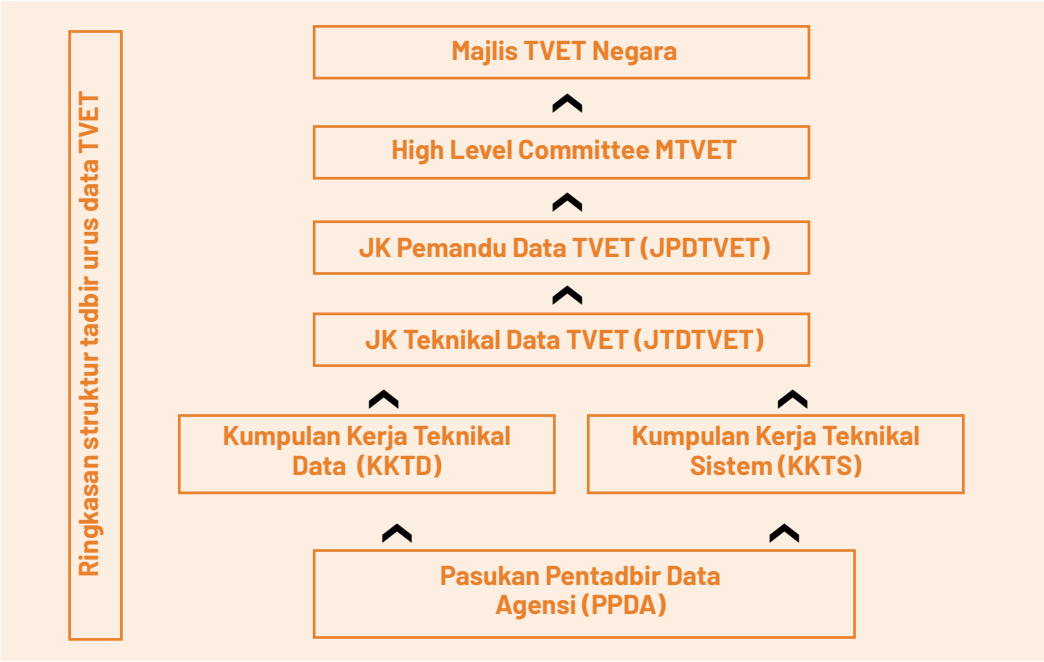
TADBIR URUS perkongsian data TVET bertindak sebagai pemudah cara dalam skop pengurusan dan perkongsian data TVET. Kecekapan tadbir urus data TVET berlandaskan instrumen perundangan dan pentadbiran semasa yang kondusif bagi menjamin platform perkongsian data yang mapan, mampan dan selamat.

2.1 Tadbir Urus Data TVET

2.1.1 Tadbir urus yang jelas dan berstruktur dalam entiti TVET adalah perlu bagi memastikan perkongsian data yang berintegriti, bersepadu dan efisien. Polisi ini dibuat bagi memperkemas proses dan memastikan amalan baik diterapkan oleh pihak-pihak yang terbabit.

2.1.2 KESUMA merupakan peneraju dalam pembangunan Data Raya TVET dengan kerjasama dari pelbagai entiti TVET yang sentiasa menyokong dan mendokong kepada kesepaduan perkongsian data TVET ini. Justeru, polisi perkongsian data TVET ini merupakan salah satu inisiatif KESUMA bagi memastikan pengurusan yang komprehensif dan holistik.

2.1.3 Tadbir urus ini melibatkan entiti TVET yang terdiri daripada beberapa jawatankuasa yang berstruktur yang dinaungi oleh Majlis TVET Negara (MTVET). Pentadbiran perkongsian data ini terdiri dari tiga (3) jawatankuasa iaitu Jawatankuasa Pemandu Data TVET (JPDTVET) yang merupakan jawatankuasa induk yang dianggotai oleh wakil dari semua entiti TVET, Jawatankuasa Teknikal Data TVET (JTDTVET) dan Kumpulan Kerja Teknikal (Data dan Sistem). Setiap entiti TVET perlu mewujudkan Pasukan Pentadbir Data Agensi (PPDA) bagi menguruskan semua perkara berkaitan data TVET di agensi masing-masing. Ringkasan struktur tadbir urus data TVET adalah seperti **Rajah 3**.



Rajah 3: Struktur Jawatankuasa dan Pasukan Data TVET

a. Majlis TVET Negara (MTVET)

Penentuan hala tuju dan strategi pelaksanaan TVET berasaskan kepada MTVET yang berperanan untuk membuat keputusan dasar peringkat negara setelah melaksanakan pertimbangan yang menyeluruh berkaitan TVET. Majlis ini juga sebagai entiti yang menyelaras kerjasama antara kementerian, agensi dan pihak-pihak lain berkaitan TVET.

b. High Level Committee (HLC)

HLC MTVET adalah entiti yang ditubuhkan melalui keputusan MTVET membincangkan isu-isu TVET yang menjadi fokus dan perlu diselesaikan termasuk Data Raya TVET. Sebarang pelan pelaksanaan, cadangan dan inisiatif perlu melalui HLC sebelum dibentangkan ke MTVET bagi tujuan pertimbangan dan kelulusan.

c. Jawatankuasa Pemandu Data TVET (JPDTVET)

JPDTVET bertanggungjawab untuk menentukan hala tuju dan strategi dasar perkongsian data TVET. Jawatankuasa ini memantau status pelaksanaan secara menyeluruh, memberikan nasihat berhubung dasar dan isu-isu semasa berkaitan perkongsian data TVET serta melaporkan kepada HLC dan MTVET. Pengerusi JPDTVET adalah KSU KESUMA dan bertanggungjawab melantik ahli dalam JPDTVET.

i. Keahlian JPDTVET

PENGERUSI	KSU, KESUMA atau pegawai yang diturunkan kuasa
AHLI-AHLI	1. Wakil tetap Kementerian TVET yang dilantik 2. Sekretariat MTVET 3. Ketua Eksekutif HRDCorp 4. Ketua Eksekutif PERKESO 5. Ketua Pegawai KWSP 6. Ketua Eksekutif TalentCorp 7. Bahagian Dasar Kesuma 8. Bahagian Undang-Undang Kesuma 9. Ahli jemputan (co-opted) berdasarkan isu/ keperluan pembentangan
KORUM MESYUARAT	Korum mesyuarat perlu melebihi separuh daripada ahli tetap atau ahli ganti.
URUSETIA	JPK

ii. Tanggungjawab JPDTVET

JPDTVET bertanggungjawab bagi perkara-perkara berikut:

1. Mengesahkan dan meluluskan sesuatu cadangan berkaitan penggunaan data TVET;
2. Meluluskan permohonan Data Raya TVET dari mana-mana pihak mengikut peringkat dan pengelasan data (data sulit dan data rahsia);
3. Meluluskan perkongsian pelaporan data TVET kepada mana-mana pihak;
4. Memudahcara kelangsungan perkongsian data secara holistik dalam ekosistem data TVET bagi kepentingan pembangunan negara;
5. Mengesahkan dan meluluskan sebarang program dan aktiviti perkongsian data merentas entiti TVET;
6. Menyelesaikan isu dan cabaran berkaitan pelaksanaan perkongsian data TVET;
7. Memutuskan tindakan yang akan diambil kepada mana-mana pihak yang didapati melanggar syarat ataupun prosedur perkongsian data;
8. Memperakukan penyelarasan kadar fi perkongsian data TVET (sekiranya ada); dan
9. Melaporkan hasil analisis Data Raya TVET kepada MTVET.

iii. Kekerapan Mesyuarat

Sekurang-kurangnya 1 kali setahun atau mengikut keperluan.

d. Jawatankuasa Teknikal Data TVET (JTDTVET)

JTDTVET bertanggungjawab dalam pemantauan pematuhan polisi perkongsian data TVET dan menyelaras program berpacukan data. Pengerusi adalah Ketua Pengarah Pembangunan Kemahiran dan bertanggungjawab melantik ahli dalam JTDTVET.

i. Keahlian JK

PENGERUSI	Ketua Pengarah Pembangunan Kemahiran atau pegawai yang diturunkan kuasa
AHLI-AHLI	1. Wakil yang dilantik dari kalangan pemilik dan pengawal data TVET di entiti TVET yang terlibat 2. Sekretariat MTVET 3. PUU JPK 4. Jabatan Perangkaan Malaysia 5. Wakil HRDCorp 6. Wakil PERKESO 7. Wakil KWSP 8. Wakil TalentCorp 9. Ahli lain boleh dijemput (co-opted) berdasarkan isu/ keperluan pembentangan
KORUM MESYUARAT	Korum mesyuarat perlu melebihi separuh daripada ahli tetap atau ahli ganti.
URUSETIA	JPK

ii. Tanggungjawab JTDTVET

Antara tanggungjawab JTDTVET adalah seperti yang berikut:

1. Merancang, menyediakan, mengenal pasti dan menyelaras strategi, prosedur serta keperluan sumber bagi pelaksanaan perkongsian data;
2. Memastikan perundangan, peraturan dan perjanjian/ Nota Kerjasama perkongsian data dipatuhi;
3. Mengenalpasti kerjasama strategik bersama agensi awam dan swasta;
4. Meneliti cadangan Kumpulan Kerja Teknikal (KKT) dan membuat pengesyoran kepada JPDTVET;
5. Memantau dan melaporkan status pelaksanaan perkongsian data TVET semasa kepada JPDTVET;
6. Memperaku program dan aktiviti bagi perkongsian data TVET peringkat nasional;
7. Mengesyorkan permohonan data sulit dan data rahsia mengikut peringkat dan pengelasan data daripada KKT;
8. Menyedia dan membentangkan laporan hasil dapatan analisis data kepada JPDTVET;
9. Mengesyorkan tindakan kepada JPDTVET sekiranya terdapat pelanggaran syarat ataupun prosedur perkongsian data;
10. Mengesahkan pengelasan data terbitan mengikut prosedur semasa; dan
11. Mencadangkan penambahbaikan (sekiranya perlu).

iii. Kekerapan mesyuarat

Sekurang-kurangnya 1 kali setahun atau mengikut keperluan.

e. Kumpulan Kerja Teknikal (KKT)

Kumpulan Kerja Teknikal (KKT) terbahagi kepada dua (2) iaitu Kumpulan Kerja Teknikal Data (KKTD) dan Kumpulan Kerja Teknikal Sistem (KKTS). KKT merupakan pasukan yang bertanggungjawab dalam membangunkan Data Raya TVET termasuk menyediakan platform, analisis dan rekabentuk, penyediaan garis panduan dan juga dasar yang melibatkan perkara-perkara teknikal. Pengerusi adalah Timbalan Ketua Pengarah JPK dan ahli dilantik oleh KP JPK.

i. Keahlian Kumpulan Kerja Teknikal

PENGERUSI	Timbalan Ketua Pengarah (Pembangunan), JPK atau pegawai yang diturunkan kuasa.
AHLI-AHLI	a. KKTD Pentadbir Data / Pemilik Data/ Pembekal Data di peringkat entiti TVET. b. KKTS Pegawai Teknikal Teknologi Maklumat di entiti TVET yang terlibat.
KORUM MESYUARAT	Korum mesyuarat perlu melebihi separuh daripada ahli tetap atau ahli ganti.
URUSETIA	JPK

ii. Tanggungjawab KKTD

Antara tanggungjawab KKTD adalah seperti yang berikut:

1. Mencadangkan prosedur yang jelas bagi permohonan perkongsian data TVET dan diangkat kepada JKTDTVET untuk kelulusan;
2. Melaksana dan menyelaras pengelasan data rahsia rasmi yang dikongsi;
3. Melaksanakan prosedur berkaitan capaian data mengikut kategori pengguna bagi menjamin keselamatan data;
4. Menyelaras dan menyediakan SOP pembersihan data;
5. Mengemaskini dan menambahbaik pelaporan statistik dan analitik data atau lain-lain laporan TVET yang berkaitan;
6. Mengesahkan prosedur kawalan dan capaian data bagi menjamin keselamatan data merentasi agensi awam dan swasta;
7. Memulakan perbincangan awal bagi kerjasama strategik dan keperluan kandungan MoU atau NoU bagi tujuan perkongsian data TVET;
8. Menyelaras keperluan dan kegunaan analisis data;
9. Menilai dan mengelaskan data terbitan mengikut prosedur semasa;
10. Mengurus dan menyelaras Kementerian atau agensi yang berdaftar dalam perkongsian data TVET;
11. Mengenal pasti data TVET merentasi entiti TVET merujuk DDSA;
12. Menetapkan dan menguatkuasakan standard dan keperluan teknikal perkongsian data;
13. Memastikan data yang diperoleh, disimpan dan diurus dengan efisien;
14. Menyelaras permohonan perkongsian data merentasi agensi awam dan swasta;
15. Menyelaras dan menyediakan prosedur pelupusan data;
16. Memastikan khidmat nasihat teknikal dan meja bantuan disediakan;
17. Memantau dan mengenalpasti isu platform perkongsian data;
18. Membuat pemantauan terhadap kualiti dan integriti data untuk menjamin ketersediaan dan kelancaran perkongsian data TVET;

19. Meneliti dan melaporkan kepada JTDTVET sekiranya terdapat pelanggaran syarat ataupun prosedur perkongsian data;
20. Menyediakan dan menyelaras kaedah dan standard perkongsian data bersama-sama agensi berkepentingan; dan
21. Mencadangkan penambahbaikan perkongsian data.

iii. Tanggungjawab KKTS adalah seperti berikut:

1. Menyelaras aktiviti teknikal perkongsian data antara agensi awam dan swasta;
2. Merancang dan menyelaras kaedah kawalan dan capaian sistem bagi menjamin keselamatan data kepada agensi awam dan swasta;
3. Merancang dan melaksanakan analisis kapasiti kepenggunaan bagi pangkalan data bersama-sama agensi awam dan swasta dilaksanakan;
4. Menyemak keperluan tambahan modul dalam Data Raya TVET;
5. Memberi khidmat nasihat teknikal dan meja bantuan;
6. Memastikan kerja-kerja back-up dan re-store data TVET dilaksanakan;
7. Memastikan kerja-kerja integrasi, migrasi, penyelenggaraan infostruktur dan infrastruktur Data Raya TVET dilaksanakan; dan
8. Menyediakan laporan bersesuaian mengikut keperluan.

iv. Kekerapan mesyuarat

Sekurang-kurangnya 1 kali setahun atau mana-mana mengikut keperluan.

f. Pasukan Pentadbir Data Agensi (PPDA)

PPDA bekerjasama dengan KKTD dan KKTS bagi memastikan kelancaran perkongsian data TVET. Skop tugas pasukan ini adalah dipantau dan diselia oleh Ketua Jabatan atau Ketua Pengarah atau Ketua Agensi masing-masing. Setiap entiti TVET perlu melantik seorang pengawal data di peringkat agensi yang akan menjadi wakil tetap dalam PPDA. Tanggungjawab PPDA adalah seperti berikut:

1. Melantik Pasukan Pengawal Data dan Sistem di peringkat agensi yang akan menjadi wakil tetap dalam KKT (Data dan Sistem).
2. Menyedia dan menyelia dokumen data, keperluan infostruktur dan infrastruktur, keperluan permohonan peruntukan dan keperluan latihan kepada kakitangan.
3. Memproses sebarang permohonan data secara in-house sekiranya ianya dimohon oleh mana-mana agensi atau individu secara kendiri.

2.2 Skop Jalinan Kerjasama Perkongsian Data TVET antara Agensi

Secara umumnya, skop jalinan kerjasama merangkumi perkara-perkara berikut:

a. Mempunyai hala tuju dan matlamat yang sama dalam perkongsian data TVET bagi membangunkan program TVET negara;
b. Menyelaras perkongsian data melalui instrumen kerjasama dalam kalangan agensi awam dan swasta;
c. Membekalkan dan menyelaras program TVET yang dikemaskini dari semasa ke semasa;
d. Membekalkan, melengkapkan maklumat dan menyelaras permohonan pelajar melalui UP_TVET;
e. Membekalkan dan menyelaras maklumat pendaftaran, persijilan dan pengajar;

f. Membekalkan dan menyelaras maklumat majikan bagi padanan kerja;
g. Menyelaras analisis data bagi keperluan nasional secara berkala;
h. Menyelaras maklumat pekerja mahir negara;
i. Menyelaras pembangunan dan penggunaan dasar dan polisi perkongsian data;
j. Menyelaras kawalan dan capaian data sentiasa dipatuhi bagi menjamin keselamatan data;
k. Menyelaras maklumat paparan di dashboard atau apa-apa platform yang relevan;
l. Menyelaras sebarang aktiviti berkaitan perkongsian data TVET dalam pelan strategik peringkat nasional; dan
m. Membekalkan dan menyelaras apa-apa maklumat yang relevan dari semasa ke semasa.

2.2.1 Keunikan kerjasama bersama Agensi Pembekal Data

Tiada kenaan fi kepada mana-mana agensi pembekal data yang membuat permohonan data. Namun, permohonan data terperingkat perlu melalui prosedur yang ditetapkan dalam polisi ini.

2.3 Pengguna Data TVET

Kategori pengguna data TVET adalah seperti berikut:

i. Pengguna Agensi Awam (G2G)

Pegawai kementerian atau jabatan kerajaan di bawah Perkhidmatan Awam Persekutuan, Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun (Persekutuan dan Negeri) dan Pihak Berkuasa Tempatan, tertakluk di bawah skop TVET.

ii. Pengguna Agensi Swasta (G2B)

Pegawai dari agensi swasta yang ditubuhkan di bawah Akta Syarikat 1965 dan organisasi swasta tempatan yang sah, tertakluk di bawah skop TVET.

iii. Pengguna awam G2C

Entiti TVET dengan rakyat Malaysia iaitu warganegara dan pemastautin tetap.

v. Penyelidik

Penyelidik yang sedang menjalankan kajian atau penyelidikan di bawah seliaan institusi pendidikan awam dan swasta dalam dan luar negara.

vi. Lain-lain

Antaranya individu atau pihak yang tidak dinyatakan di atas.

2.4 Perkongsian dan Pengintegrasian Data TVET

2.4.1 Tatacara Perkongsian dan Pengintegrasian

Tatacara perkongsian dan pengintegrasian ini adalah selaras dengan Dasar Perkongsian Data Nasional dan Dasar Perkongsian Data Sektor Awam. Mana-mana pengguna perlu mendaftar sebagai pengguna pangkalan Data Raya bagi mendapatkan akses kepada data TVET. Terdapat beberapa peringkat dalam perkongsian atau pengintegrasian data seperti berikut:

i. Antara individu dengan pangkalan Data Raya TVET

Pada peringkat individu (pengajar, pelajar, pemohon) yang melibatkan data peribadinya disimpan dan digunakan oleh entiti TVET, dan dikongsi atau diintegrasi kepada pangkalan Data Raya TVET sepertimana peruntukan dalam PDPA 2010 perlu dipatuhi.

ii. Antara entiti dalam ekosistem TVET

Pada peringkat entiti dalam ekosistem TVET, semua entiti TVET perlu mematuhi tatacara perkongsian dan pengintegrasian data. Permohonan data terbuka boleh diakses di platform pangkalan data secara dalam talian. Manakala permohonan perkongsian data terperingkat perlu dikemukakan kepada JPK yang mana permohonan tersebut disemak oleh data KKTD dan dibentangkan dalam JTDTVET sebelum diluluskan dalam JPDTVET.

iii. Antara KESUMA dengan pihak luar ekosistem TVET.

Mana-mana permohonan perkongsian data dari pihak luar ekosistem TVET seperti majikan, industri dan pertubuhan kepada KKTD. Permohonan tersebut perlu disahkan oleh JTDTVET. Maklumat perkongsian data adalah melalui MoU atau apa-apa dokumen perjanjian boleh ditandatangani untuk perkongsian atau pengintegrasian dalam skop bidang kerjasama, perlindungan harta intelek, perlindungan data peribadi, kerahsiaan dan tempoh kerjasama. Perjanjian perkongsian atau pengintegrasian data menjelaskan terma dan syarat penggunaan data, sah untuk tempoh masa tertentu, dan memberikan kesan perundangan jika tidak dipatuhi. Perkongsian data adalah tertakluk kepada kenaan fi dan caj kepada mana-mana permohonan perkongsian data kepada pihak luar selain entiti TVET.

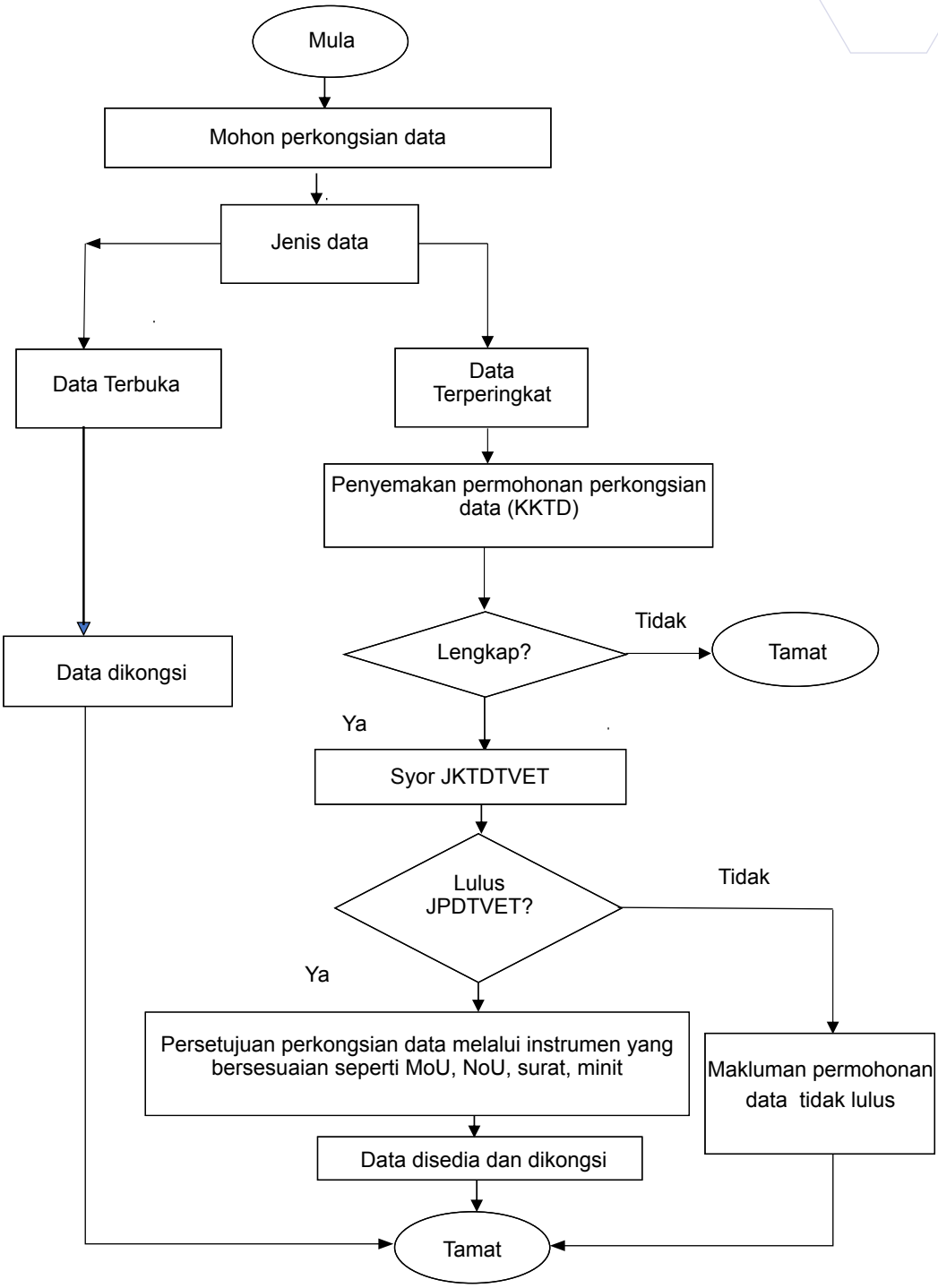
2.4.2 Prosedur Permohonan Perkongsian Data Terperingkat

i. Prosedur permohonan perkongsian data terperingkat adalah seperti Rajah 4 di bawah. Sebarang permohonan perkongsian data terperingkat secara bertempoh atau one off perlu dikemukakan kepada KESUMA (permohonan secara manual atau melalui sistem) dan permohonan tersebut perlu di bawa ke KKTD.

ii. Mana-mana permohonan yang tidak lengkap atau tidak jelas akan dikembalikan semula kepada pemohon. Kelulusan permohonan data terperingkat hendaklah mematuhi prosedur yang telah ditetapkan oleh JTDTVET. JPDTVET akan memberikan kelulusan bagi sebarang permohonan perkongsian data terperingkat sama ada secara bertempoh atau one off.

iii. Permohonan perkongsian data terperingkat perlu ditimbang dengan sewajarnya oleh JPDTVET dan dokumen perkongsian data akan dikeluarkan sekiranya data terperingkat tersebut dipersetujui untuk dikongsi dan terma bayaran akan dikemukakan sekiranya bercaj.

iv. Mana-mana permohonan data yang telah diluluskan akan dikeluarkan surat atau minit atau MoU atau NoU dan mana-mana data terperingkat yang tidak boleh dikongsi akan dimaklumkan kepada pemohon.



Rajah 4 : Prosedur Permohonan Perkongsian Data

2.4.3 Kaedah Penyaluran Data

Mekanisme pengintegrasian data antara entiti TVET melalui infostruktur dan infrastruktur pengintegrasian data yang optimum. JPK bertanggungjawab memastikan pengurusan pengintegrasian berjalan dengan lancar dengan menggunakan platform perkongsian data kerajaan MyGDX atau pembangunan API bagi pengintegrasian data yang dikenalpasti seperti Jadual 3.

Jadual 3: Kategori Permohonan dan Kaedah Pengintegrasian Data

Bil.	Kategori Permohonan	Kaedah Pengintegrasian Data
1.	One-off (sekali sahaja)	a. Melalui e-mel – fail dalam format yang bersesuaian (cth: txt, xls dan csv) b. Lain-lain kaedah yang bersesuaian
2.	Berkala	a. Integrasi melalui API atau Web Services b. Melalui e-mel – fail dalam format yang bersesuaian (cth: txt, xls dan csv) c. Lain-lain kaedah yang bersesuaian

Pengintegrasian data adalah secarai API dan dokumen IDD (Lampiran A dan Lampiran B) hendaklah diisi bagi rujukan dan penerangan proses integrasi secara terperinci.

2.4.4 Tanggungjawab pemohon adalah seperti berikut:

i. Data yang telah diluluskan hanya boleh digunakan bagi tujuan permohonan yang telah ditetapkan dalam borang permohonan;
ii. Sentiasa menjaga kerahsiaan, keselamatan dan integriti data yang dibekalkan;
iii. Data yang telah diluluskan tidak boleh disebarkan kepada mana-mana pihak yang tidak diberi kebenaran melalui apa jua cara sekalipun;
iv. Sebarang terbitan atau pelaporan yang menggunakan data diluluskan hendaklah dinyatakan sumbernya;
v. Data yang telah diluluskan tidak boleh dimanipulasi sehingga menjejaskan maklumat data asal; dan
vi. Pemohon adalah bertanggungjawab terhadap sebarang kemungkinan kesilapan interpretasi berkaitan dengan penilaian dan pentafsiran data.

2.4.5 Pemohon yang didapati melanggar mana-mana perkara dalam 2.4.4 boleh diambil tindakan di bawah akta berkaitan yang sedang berkuatkuasa.

2.5 Etika Pengurusan Data Berkesan dan Perundangan Kondusif

2.5.1 Etika pengurusan data memerlukan peruntukan perundangan dan peraturan yang perlu dipatuhi bagi perkongsian data yang berkesan seperti berikut:

a. Akta Rahsia Rasmi 1972 [Akta 88];
b. Akta Perlindungan Data Peribadi 2010;
c. Akta Keselamatan Siber 2024 [Akta 854];
d. Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993 [P.U (A) 395/1993];
e. Dasar Perkongsian Data Nasional, Kementerian Digital 2022;
f. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bil.2 Tahun 2021 – Dasar Perkongsian Data Sektor Awam;
g. Pekeliling Arahan Keselamatan Terhadap Dokumen Geospatial Terperingkat;
h. Arahan Keselamatan [Semakan dan Pindaan 2017]; dan
i. Tertakluk pada mana-mana perundangan sedia ada yang sedang berkuat kuasa.

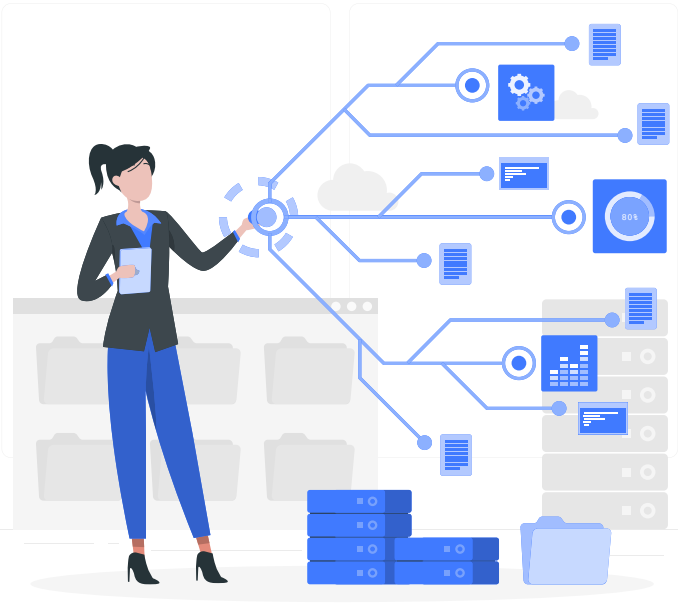
2.5.2 Mana-mana individu yang melanggar mana-mana perkara 2.5.1 akan dikenakan tindakan di bawah perundangan yang dinyatakan.

2.6 Pangkalan Data Raya TVET

2.6.1 Pangkalan Data Raya TVET merupakan pemangkin dalam sistem penyampaian perkhidmatan berkaitan TVET secara menyeluruh bagi memudah cara perkongsian data yang terkini dan sahih merentas agensi. lanya juga dapat mengurangkan pertindihan dalam usaha pengumpulan data yang menjimatkan masa, tenaga dan kos pembangunan aplikasi.

2.6.2 Secara umumnya, pangkalan Data Raya TVET mempunyai ciri-ciri seperti berikut:

2.6.3 Pangkalan Data Raya TVET ini diselia dan diselenggara oleh JPK, KESUMA. Secara khususnya, skop spesifik JPK berkaitan pangkalan Data Raya TVET adalah seperti berikut:



i. **Memantau dan mengurus supaya platform sentiasa tersedia untuk digunakan;**

ii. **Memastikan dan menjamin keselamatan operasi platform dan tugasan teknikal bersama-sama agensi awam dan swasta;**

iii. **Memberikan khidmat nasihat teknikal kepada agensi berkaitan yang menggunakan platform;**

iv. **Menguruskan dan menyelaras data dengan efisien bersama-sama agensi awam dan swasta dalam platform yang sama; dan**

v. **Menyediakan infostruktur dan infrastruktur pemboleh daya perkongsian data yang lengkap, mencukupi dan selamat.**

2.7 Kegunaan Data Raya TVET

Kegunaan Data Raya TVET adalah seperti berikut:

i. Pemohon dapat akses maklumat program dan institusi yang menawarkan program secara holistik.

ii. Profil pengajar TVET dapat diselaraskan secara berpusat bagi meningkatkan kompetensi pengajar.

iii. Membolehkan para graduan TVET untuk membuat carian pekerjaan yang bersesuaian dengan jurusan atau bidang yang diambil.

iv. Majikan turut boleh mengenalpasti calon pekerja yang bersesuaian bagi memenuhi kebolehkerjaan.

v. Kegunaan perkongsian data adalah bagi tujuan analisis seperti berikut:

   a. Keperluan Pemegang Taruh
      Data yang diperlukan untuk memenuhi keperluan dan kehendak pemegang taruh.

   b. Perancangan dan Pembuatan Keputusan
      Data dapat membantu pemegang taruh membuat keputusan atau merangka dasar-dasar baharu berdasarkan analisa dan kajian seperti membangunkan pekeliling perkhidmatan.

   c. Pemantauan Prestasi
      Data untuk melaksanakan proses pemantauan prestasi agensi.

d. Kesinambungan Proses Bisnes (Business Process Continuity)
Ketersediaan data dapat dikekalkan dan dilindungi walaupun terdapat sebarang ancaman dan cabaran yang tidak dijangka.

e. Kelestarian data
Data kekal relevan, dapat diguna, diakses dan dijaga integriti sepanjang kitaran hayat data tersebut.

f. Analitis Data
Analitis data merupakan proses untuk menganalisis data TVET yang berinovasi bagi mendapatkan pengetahuan dalam membantu membuat keputusan. Perkongsian data antara setiap agensi awam dan swasta adalah diperlukan bagi membolehkan data dianalisis secara holistik dan bersepadu. Penganalisisan data TVET bagi agensi sektor awam dan sektor swasta ini membolehkan:
   i. Penggunaan data dapat dioptimumkan dengan kesetaraan maklumat, sahih dan lengkap;
   ii. Meningkatkan kualiti penyampaian dan perkhidmatan kepada rakyat; dan
   iii. Menghasilkan maklumat dan pengetahuan melalui analisis data yang berbentuk deskriptif, diagnostik, prediktif dan preskriptif yang dapat membantu agensi sektor awam dan sektor swasta bagi sesuatu keputusan dan pembentukan dasar yang baharu.

BAB 3:
PERLINDUNGAN DAN KESELAMATAN

3.0 PERLINDUNGAN DAN KESELAMATAN

3.1 Keselamatan Data Raya TVET

Keselamatan Data Raya TVET bertujuan menjamin keselamatan dan ketersediaan data TVET dalam pelaksanaan perkongsian data. Terdapat lima (5) asas keselamatan Data Raya TVET iaitu kerahsiaan, integriti, ketersediaan, tidak boleh disangkal dan sahih.

a. Kerahsiaan

Semua pihak yang terlibat dalam perkongsian Data Raya TVET hendaklah menjaga kerahsiaan Data Raya TVET mengikut instrumen perundangan dan pentadbiran yang berkuatkuasa dari semasa ke semasa.

b. Integriti

Data Raya TVET yang dimiliki, disediakan atau ditadbir oleh semua pihak yang terlibat perlu tepat, lengkap, terkini dan berpunca daripada sumber yang sahih. Data Raya TVET tidak boleh dikongsi dengan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran pihak bertanggungjawab.

c. Ketersediaan

Data Raya TVET hendaklah boleh diakses pada bila-bila masa oleh mana-mana pihak yang sah dan dibenarkan sahaja.

d. Tidak Boleh Disangkal

Sumber Data Raya TVET hendaklah dari punca yang sah dan tidak boleh disangkal. Semua pihak yang terlibat perlu mengambil langkah keselamatan dan membuat langkah kontingensi sekiranya terdapat ketirisan dalam perkongsian data.

e. Kesahihan

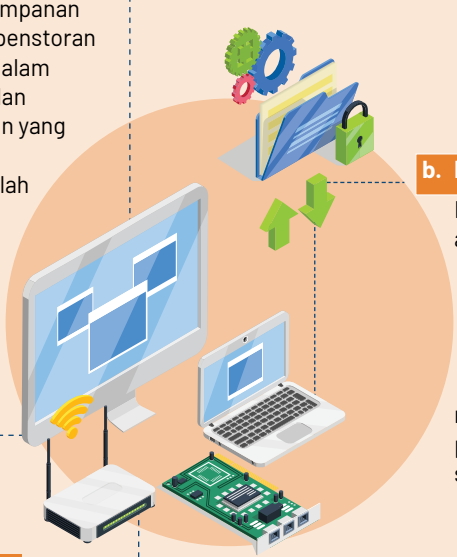
Setiap transaksi perkongsian Data Raya TVET hendaklah dilaksanakan secara sah sebagaimana yang dipersetujui oleh semua pihak yang terlibat.

3.1.1 Pemprosesan Data Raya TVET

Semua pihak yang terlibat hendaklah memastikan keselamatan Data Raya TVET di semua peringkat pemprosesan data dan perlu mengambil langkah yang telah ditetapkan di dalam akta, pekeliling, garis panduan, prosedur dan dasar semasa termasuk dalam pemilihan teknologi yang digunakan bagi melaksanakan perlindungan ketirisan data. Keselamatan dan langkah perlindungan data perlu diambil kira di setiap pemprosesan data yang terdiri daripada empat (4) peringkat seperti yang berikut:

a. Data-dalam-simpanan

Pembekal data berupaya menyimpan data-dalam-simpanan dalam mana-mana media penstoran yang mana data tersebut dalam keadaan tidak digunakan dan statik. Ciri-ciri keselamatan yang perlu diaplikasikan kepada data-dalam-simpanan adalah seperti penyulitan, multi-factor authentication dan kawalan akses capaian secara fizikal serta secara digital atau apa-apa kaedah yang bersesuaian.



b. Data-dalam-pergerakan

Data-dalam-pergerakan atau data-in-motion merujuk data yang sedang bergerak atau data yang sedang dipindahkan perlu dalam keadaan selamat dengan menggunakan mana-mana kaedah pemindahan data yang sesuai.

d. Data-dalam-arkib

Data-dalam-arkib merujuk Data Raya TVET yang tidak digunakan selepas tempoh aktif yang telah ditetapkan iaitu 10 tahun mengikut tatacara pelupusan digital yang berkuatkuasa.

c. Data-dalam-penggunaan

Semua pihak yang terlibat dengan Data Raya TVET perlu berhati-hati dalam pengendalian data yang melibatkan proses mencipta, mengemaskini atau memadamkan data tersebut. Pembekal data dan pentadbir data perlu melaksanakan ciri-ciri keselamatan pada medium capaian dan pengesahan serta pengurusan identiti yang kukuh.

3.1.2 Perkongsian Data Raya TVET

a. Data Raya TVET perlu dilindungi daripada dicerobohi, disalah guna atau dicapai secara tidak sah bagi menjamin keselamatannya di sepanjang kitaran hayat Data Raya TVET. Data Raya TVET yang didedahkan kepada pihak yang tidak dibenarkan secara sengaja atau tidak sengaja boleh memberikan kesan serius kepada organisasi dan menjejaskan keselamatan dan kedaulatan negara.

b. Data Raya TVET juga hendaklah dilindungi daripada ancaman keselamatan siber seperti penggodaman, pencerobohan sistem, serangan virus serta ancaman keselamatan fizikal data seperti pencerobohan (pecah masuk), kecurian, kebakaran ke atas premis dan sebagainya. Pengendalian data rahsia rasmi (sekiranya ada) dalam persekitaran ICT hendaklah mematuhi tatacara yang ditetapkan di dalam Arahan Keselamatan (Semakan dan Pindaan 2017) Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (Chief Government Security Officer- CGSO) serta Pelan Keselamatan Siber yang berkuatkuasa di bawah agensi yang menyediakan platform perkongsian data.

3.2 Keselamatan Pangkalan Data Raya TVET

Keselamatan dan perlindungan Data Raya TVET perlu diambil kira di setiap peringkat pemprosesan data. Data-data perlu disimpan dalam pangkalan data yang ditempatkan di lokasi dan persekitaran selamat serta mempunyai kawalan capaian terhad untuk melindungi data-dalam-simpanan.

3.2.1 Data TVET hendaklah disimpan dan diproses di dalam pangkalan Data Raya TVET dan ditadbir oleh agensi penyelaras.

3.2.2 Agensi penyelaras hendaklah melaksanakan penilaian risiko keselamatan terhadap aplikasi, perisian, perkakasan, pelayan, rangkaian, pangkalan data, sumber manusia, proses dan prosedur bagi mengukur dan menganalisis tahap risiko. Seterusnya mengambil tindakan merancang dan mengawal risiko yang dikenal pasti yang dipertanggungjawab di bawah KKTD dan KKTS.

3.2.3 Pemindahan dan pemprosesan Data Raya TVET dilaksanakan secara berpusat dengan kawalan capaian terhad serta jejak audit capaian diaktifkan bagi merekodkan aktiviti capaian data yang dipertanggungjawab di bawah KKTD dan KKTS.

3.2.4 Perlindungan kebocoran data (data leakage protection) hendaklah diterapkan bagi pengesanan awal aktiviti ketirisan data dan maklumat secara elektronik. Sekiranya berlaku ketirisan data, tindakan mitigasi segera perlu diambil.

3.2.5 Agensi penyelaras perlu memastikan keselamatan sistem dan Data Raya TVET terjamin daripada aktiviti ancaman siber dengan memasang peralatan keselamatan ICT yang lengkap dan terkini seperti Firewall, Intrusion Prevention System (IPS), Network Management System (NMS), Antivirus, E-mail anti-spam, Web Application Firewall (WAF) atau mana-mana teknologi yang bersesuaian.

3.2.6 Agensi penyelaras hendaklah melaksanakan penilaian Security Posture Assessment (SPA) secara berkala bagi memastikan tahap keselamatan dipantau secara berterusan.

3.2.7 Agensi penyelaras hendaklah memastikan perisian yang digunakan sentiasa dikemaskini.

3.2.8 Agensi penyelaras hendaklah memastikan salinan data dibuat secara berkala di pusat data dan pusat pemulihan bencana. Pusat pemulihan bencana perlu dibangunkan bagi menghadapi sebarang risiko kegagalan di pusat data.

3.3 Pengurusan Insiden Keselamatan Siber

Sekiranya terdapat penemuan insiden keselamatan siber, agensi penyelaras Data Raya TVET perlulah melaksanakan pengurusan insiden keselamatan siber berdasarkan pekeliling yang sedang berkuatkuasa iaitu Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam. Agensi penyelaras juga perlu bekerjasama dengan Computer Security Incident Response Team (CERT), KESUMA bagi pengurusan insiden keselamatan siber.

3.3.1 Undang-Undang Berkaitan Insiden Keselamatan Siber

Semua pihak yang terlibat dalam pengurusan Data Raya TVET bertanggungjawab sepenuhnya untuk menjaga keselamatan dan kerahsiaan Data Raya TVET mengikut peraturan dan akta dari semasa ke semasa tidak terhad kepada:

a. Akta Rahsia Rasmi 1972 (Akta 88).
b. Akta Jenayah Komputer 1997 (Akta 563).
c. Akta Komunikasi dan Multimedia 1998 (Akta 588).
d. Akta Perlindungan Data Peribadi 2010 (Akta 709).
e. Akta Keselamatan Siber 2024 [Akta 854].

4.0 PENUTUP

Polisi Perkongsian Data Raya TVET ini merupakan satu polisi yang perlu dirujuk oleh semua pihak yang terlibat bagi merealisasikan perkongsian data TVET yang eksklusif, telus, selamat, efisien dan bersepadu.

LAMPIRAN

Lampiran A

INTERFACE DESCRIPTION DOCUMENT (IDD)

MIGRASI DAN PEMBANGUNAN API

<NAMA SERVIS>

PROJEK PENINGKATAN NATIONAL REGISTRIES (MyGDX 2.0)

JABATAN DIGITAL NEGARA

Disediakan oleh:

< Nama Agensi Pembekal >

Tarikh Disediakan:

xx/xx/202x

NAMA AGENSI	**:**	**xxxx**
NAMA AGENSI INDUK	**:**	**xxxxx**
TARIKH DOKUMEN	**:**	**xxxx**
VERSI DOKUMEN	**:**	**xxxx**

KETERANGAN DOKUMEN

Dokumen ini menentukan keperluan pelaksaan proses migrasi dan pembangunan API.

Melalui dokumen ini, migrasi dan pembangunan API boleh mendapatkan maklumat terperinci berkenaan matlamat dan memahami keperluan pelaksaan proses migrasi yang akan dibangunkan.

SEMAKAN DOKUMEN

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Disediakan Oleh			
Disemak Oleh			
Disahkan Oleh			

PENGESAHAN DOKUMEN OLEH <AGENSI>

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Disemak Oleh			
Disahkan Oleh			

PENGESAHAN DOKUMEN OLEH MYGDX

Aktiviti	Nama/Jawatan	Tandatangan	Tarikh
Diluluskan Oleh			

KAWALAN DOKUMEN

Versi	Tarikh	Ringkasan Pindaan	Penyedia

KANDUNGAN

SENARAI AKRONIM

Terma	Keterangan
API	*Application Programming Interface*
DDSA	Data *Dictionary* Sektor Awam
IDD	*Interface Description Document*
JDN	Jabatan Digital Negara
MyGDX	*Malaysian Government Central Data Exchange*
URL	*Uniform Resource Locator*
UXP	*Unified eXchange Platform*

SENARAI TERMA/ISTILAH

Terma/Istilah	Definisi
Agensi	Sesebuah organisasi yang meliputi pelbagai sektor seperti awam, swasta, badan berkanun dan institusi bukan kerajaan yang lain, yang mana ianya mempunyai kepentingan yang kukuh untuk melanggan dan menggunakan perkhidmatan yang disediakan oleh MyGDX.
Agensi Pembekal	Agensi yang membekalkan data dan memberi kebenaran kepada agensi lain untuk menggunakan data tersebut.

SUMBER RUJUKAN

Bil.	Keterangan
1.	Dokumen Pelan Migrasi dan Spesifikasi API

1 PENGENALAN MENGENAI DOKUMEN

Dokumen ini merupakan salah satu keperluan utama dalam mendapatkan maklumat terperinci berkaitan perlaksanaan aktiviti pembangunan dan migrasi API bagi projek Peningkatan National Registries – *Malaysian Government Central Data Exchange* (MyGDX).

1.1 Objektif

Objektif dokumen *Interface Description Document* (IDD) ini adalah untuk menerangkan struktur dan format data yang terlibat dalam migrasi dan pembangunan API bagi agensi pembekal dalam projek *Malaysian Government Central Data Exchange* (MyGDX).

Dokumen IDD perlu dipersetujui oleh agensi pembekal bagi memastikan semua struktur dan format data yang diperlukan adalah menepati keperluan migrasi dan pembangunan API.

1.2 Skop

Keperluan pembangunan dan migrasi API yang dihuraikan dalam dokumen ini adalah mengenai keterangan *interface* API dan juga data format *request* dan *response* bagi setiap API yang akan terlibat dalam pembangunan dan migrasi API ini.

1.3 Organisasi Dokumen

Dokumen ini telah disediakan mengikut susunan seperti yang diterangkan dalam Jadual 1 di bawah.

Jadual 1 Organisasi Dokumen

BIL.	SEKSYEN	PENERANGAN
1.	Pengenalan Mengenai Dokumen	Bahagian ini menerangkan secara ringkas berkenaan dokumen ini.
2.	Keterangan *Interface*	Bahagian ini akan menerangkan mengenai maklumat *interface*.

2 KETERANGAN *INTERFACE*

2.1 <NAMA SERVIS>

2.1.1 Keterangan *Interface*

Nama Servis	<Nama Servis>
Keterangan Servis	Servis ini untuk ….
Jenis Data	Contoh: Sulit, Terbuka
Agensi Pembekal	Contoh: JDN
Kaedah Integrasi	SOAP Atau REST
Servis ID	<KodAgensi>-<NamaSistemPembekal>-<PilihanCRUD>-<JenisMaklumat> Contoh: JDN-DDSA-R-KodTarafKahwin
Method	POST/GET
URL API	
Authentication	Certificate

2.1.2 Senarai Agensi Pengguna

Bil.	Nama Agensi Pengguna	memberCode	subsystemCode
1.	Contoh: Jabatan Kebajikan Masyarakat	Contoh: JKM	Contoh: SMOKU

2.1.3 Format dan *Standard* API MyGDX

Berikut merupakan Standard *Header* untuk UXP bagi jenis kaedah integrasi SOAP yang baharu:

Standard Header *Format untuk SOAP*			
Parameter Input	**Keterangan**	**Header/Body**	**Value**
Maklumat Agensi Pengguna			
xRoadInstance	RoadInstance Agensi Pengguna	Header	MYGDX
memberClass	memberClass Agensi Pengguna	Header	GOV
memberCode	memberCode Agensi Pengguna	Header	<KodAgensiPengguna>
subsystemCode	subsystemCode Agensi Pengguna	Header	<KodSistemAgensiPengguna>
Maklumat Agensi Pembekal			
xRoadInstance	RoadInstance Agensi Pembekal	Header	MYGDX
memberClass	memberClass Agensi Pembekal	Header	GOV
memberCode	memberCode Agensi Pembekal	Header	<KodAgensiPembekal>
subsystemCode	subsystemCode Agensi Pembekal	Header	<KodSistemAgensiPembekal>
serviceCode	serviceCode Agensi Pembekal	Header	<ServisID>
serviceVersion	Service Version	Header	v1

2.1.3.1 Contoh *Header* Mesej (SOAP)

```
<soapenv:Header>
    <xro:client iden:objectType="SUBSYSTEM">
      <iden:xRoadInstance>MYGDX</iden:xRoadInstance>
      <iden:memberClass>GOV</iden:memberClass>
      <iden:memberCode>JDN</iden:memberCode>
      <!--Optional:-->
      <iden:subsystemCode>GOSG</iden:subsystemCode>
    </xro:client>
    <xro:service iden:objectType="SERVICE">
      <iden:xRoadInstance>MYGDX</iden:xRoadInstance>
      <iden:memberClass>GOV</iden:memberClass>
      <iden:memberCode>JDN</iden:memberCode>
      <!--Optional:-->
      <iden:subsystemCode>DDSA</iden:subsystemCode>
<iden:serviceCode>JDN-DDSA-R-
KodTarafKahwin</iden:serviceCode>
      <!--Optional:-->
      <iden:serviceVersion>v1</iden:serviceVersion>
    </xro:service>
    <xro:protocolVersion>4.0</xro:protocolVersion>
  </soapenv:Header>
```

Standard Header Format *untuk UXP REST-API*		
Paramater Name	**Data Structure**	**Value**
Maklumat Agensi Pengguna		
UXP-client	InstanceName/MemberClass/MemberName/ Subsystem/	MYGDX/GOV/<KodAgensi Pengguna>/<KodSistemA gensiPengguna>
Maklumat Agensi Pembekal		
UXP-Service	InstanceName/MemberClass/MemberName/ Subsystem/ServiceName/Version	MYGDX/GOV/<KodAgensi Pembekal>/<KodSistemA gensiPembekal>/<ServisI D>/v1

2.1.3.2 Contoh Header Mesej (REST)

```
“header":{
        "UXP-client":"MYGDX/GOV/JDN/GOSG",
        "UXP-Service":" MYGDX/GOV/JDN/DDSA/JDN-DDSA-R-KodTarafKahwin"
    }
```

2.1.4 Data Format (Request)

Bil	Nama Medan	Keterangan	Jenis Data	Header/ Body
1.				

2.1.5 Data Format (Response)

Bil	Nama Medan	Keterangan	Jenis Data	Header/ Body
1.				
2.				

2.1.5.1 Contoh Response Mesej (SOAP)

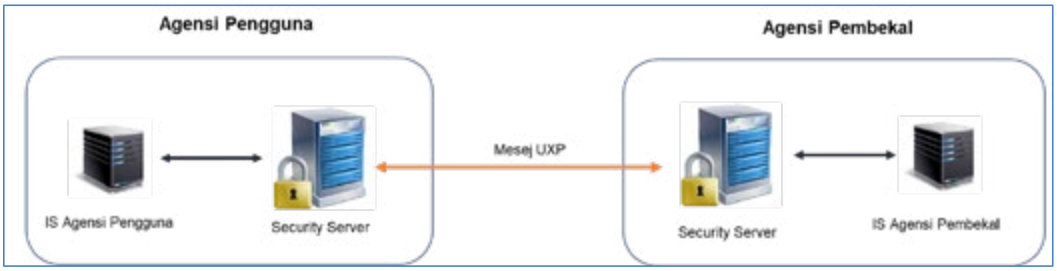
2.1.6 *Error Handling*

Bagi maklumat *error handling* boleh rujuk pada **Lampiran 1**.

3 LAMPIRAN

3.1 LAMPIRAN 1: *Error Handling*

3.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat



Rajah 1: Pertukaran Mesej UXP

Semasa pertukaran mesej di antara *Security Server* Agensi Pengguna dan *Security Server* Agensi Pembekal, ralat boleh berlaku dan mesej ralat ini akan disimpan di dalam log di *Security Server*.

Ralat yang dijana oleh *Security Server* mempunyai struktur dan informasi yang konsisten. Struktur mesej ralat adalah berbeza mengikut kepada kaedah servis yang digunakan samada REST atau SOAP.

3.1.1.1 Format atau Struktur Kod Ralat dan Mesej Ralat (SOAP)

Bagi kaedah SOAP berikut merupakan sturktur dan format ralat yang akan dijana oleh *Security Server*. Ralat yang dijana adalah dalam format XML:

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
     <faultcode>Server.ClientProxy.ServiceFailed.MissingBod
y</faultcode>
      <faultstring>Malformed SOAP message: body
missing</faultstring>
      <faultactor />
      <detail>
        <faultDetail>f31e7451-f0ac-48f6-9f05-
1f0459e48eea</faultDetail>
      </detail>
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

(1) <faultcode> akan menunjukkan dimana punca ralat berlaku.

   i. “Server.ClientProxy” dan “Client”membawa maksud ralat yang berlaku adalah di *Security Server* Agensi Pengguna.

   ii. “Server.ServerProxy” membawa maksud ralat yang berlaku adalah di *Security Sever* Agensi Pembekal.

(2) <faultString> akan menunjukkan punca ralat dengan lebih terperinci.

(3) <faultDetail> merupakan pengenal unik bagi mesej ralat yang diterima.Pengenal unik ini boleh digunakan bagi tujuan carian mesej ralat di log *proxy* (var/log/uxp/proxy.log atau dari Logs di Security Server)

3.1.1.2 Format atau Struktur Kod Ralat dan Mesej Ralat (REST)

Bagi kaedah REST berikut merupakan sturktur dan format ralat yang akan dijana oleh *Security Server*. Ralat yang dijana adalah di dalam format text:

Security server has no valid authentication certificate

Di HTTP *Headers* akan mempunyai kod ralat (UXP-FaultCode), mesej ralat (UXP-FaultString) dan keterangan ralat (UXP-FaultDetail).

Uxp-*FaultCode*: Server.ClientProxy.SslAuthenticationFailed

Uxp-*FaultString*: *Security server has no valid authentication certificate*

Uxp-*FaultDetail*: f31e7451-f0ac-48f6-9f05-1f0459e48eea

(1) Uxp-*FaultCode* akan menunjukkan dimana punca ralat berlaku.
   i. "Server.ClientProxy" dan "Client"membawa maksud ralat yang berlaku adalah di *Security Server* Agensi Pengguna.
   ii. "Server.ServerProxy" membawa maksud ralat yang berlaku adalah di *Security Sever* Agensi Pembekal.

(2) Uxp-*FaultString* akan menunjukkan punca ralat dengan lebih terperinci.

(3) Uxp-FaultDetail merupakan pengenal unik bagi mesej ralat yang diterima.Pengenal unik ini boleh digunakan bagi tujuan carian mesej ralat di log *proxy* (var/log/uxp/proxy.log atau dari Logs di Security Server)

3.1.2 Ralat Daripada Sistem Agensi Pengguna

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
405 Not Found	1. Ia menunjukkan bahawa URL yang anda gunakan dalam permintaan anda tidak wujud pada pelayan.	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
	2. Walaupun ini adalah ralat 404, yang biasanya bermaksud sesuatu pada bahagian *klien* adalah salah, ini juga boleh menunjukkan masalah pelayan. Kadangkala URL API berubah selepas kemas kini versi, tetapi kadangkala ia berubah kerana ada masalah pada pelayan. 3. Tindakan terbaik ialah menyemak sama ada anda tidak mempunyai kesilapan menaip dalam kod pelanggan anda sebelum menyemak sama ada API mempunyai masalah.	
401 *Unauthorized*	1. Kod status ini bermakna anda belum lagi mengesahkan terhadap API. API tidak tahu siapa anda dan oleh itu ia tidak akan melayani anda. 2. Untuk kebanyakan API, anda perlu mendaftar dan mendapatkan kunci API. Kunci ini kemudiannya digunakan dalam medan *header* HTTP apabila anda menghantar permintaan, memberitahu API siapa anda.	
403 *Forbidden*	1. Status terlarang menunjukkan bahawa anda tidak mempunyai kebenaran untuk meminta URL tersebut. Perbezaan kepada status Tanpa Kebenaran ialah anda telah disahkan, tetapi pengguna atau peranan yang anda sahkan tidak dibenarkan membuat permintaan. 2. Ini juga berlaku apabila anda mempunyai isu pengesahan, seperti apabila menggunakan kunci API yang salah atau cuba mengakses ciri yang tidak dibenarkan oleh pelan langganan anda.	
400 *Bad Request*	1. Status permintaan buruk ialah salah satu mesej *error* yang paling generik. Ini menunjukkan bahawa anda melakukan sesuatu yang salah dalam permintaan anda. 2. Anda perlu menyemak dokumen. Anda mungkin kehilangan pertanyaan atau *body field* dalam permintaan, atau *header* mungkin salah. Mungkin juga sesetengah data permintaan anda mungkin mempunyai format yang salah.	
429 *Too Many Requests*	1. Kebanyakan pelan langganan API mempunyai had: lebih murah pelan, lebih sedikit permintaan sesaat	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
	dibenarkan untuk kunci API anda. Jika anda menghantar terlalu banyak permintaan dalam masa yang singkat, pertimbangkan untuk mengecilkannya dalam pelanggan anda. Status ini juga boleh menunjukkan bahawa anda mencapai had harian, mingguan atau bulanan pada akaun anda. 2. Kadangkala API kelihatan seperti sesuai sehingga anda melihat hadnya, dan tiba-tiba ia tidak berfungsi untuk kes penggunaan anda lagi. Semak bahagian langganan API anda sebelum menyepadukan jika tidak, anda mungkin menghadapi masalah beberapa minggu atau bulan selepas menyepadukan API.	
500 *Internal Server Error*	1. Status ini boleh bermakna apa sahaja, tetapi ia biasanya menunjukkan *server* API *error*. Ia mungkin disebabkan oleh sesuatu yang berkaitan dengan permintaan. Semak semula dokumen untuk memastikan anda melakukan semuanya dengan betul seperti *query fields, body fields, headers, format*, etc. 2. Jika itu tidak menyelesaikan masalah, ia mungkin juga berkaitan dengan kemas kini API yang memperkenalkan kod buggy, atau data yang dimuatkan oleh API daripada perkhidmatan *upstream*. Dalam kes itu, satu-satunya punca tindakan anda ialah menghubungi sokongan API.	
502 *Bad Gateway*	1. Status ini memberitahu anda bahawa pelayan yang anda panggil bukanlah pelayan API sebenar, tetapi gerbang atau proksi. Pelayan proksi cuba memanggil pelayan API atas nama anda. Status juga menunjukkan bahawa pelayan API tidak menjawab. Ini mungkin berkaitan dengan masalah rangkaian, atau hanya kerana *server* API tidak berfungsi. 2. Masalah ini biasanya hanya sementara dan harus diselesaikan oleh penyedia API, tetapi anda perlu menghubungi sokongan jika ia berterusan.	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
503 *Service Unavailable*	1. Status perkhidmatan tidak tersedia bermakna pelayan terlebih muatan. Terlalu banyak permintaan API telah dihantar dan kini API tidak dapat mengendalikannya lagi. Masalah ini selesai dengan sendirinya apabila pelanggan menghantar lebih sedikit permintaan, tetapi ini juga boleh bermakna penyedia API tidak merancang sumber yang mencukupi untuk semua pelanggannya. 2. Jika ia sesuai dengan kes penggunaan anda, anda boleh menjadikan pelanggan anda lebih berdaya tahan terhadap *error* ini dengan menunggu untuk menghantar lebih banyak permintaan. Tetapi jika *error* muncul, anda perlu menghubungi pembekal API.	
501 *Not Implemented*	1. Status tidak dilaksanakan adalah berkaitan dengan kaedah HTTP yang anda gunakan untuk meminta URL. Anda boleh mencuba kaedah lain untuk membuat permintaan. 2. Biasanya, permintaan dengan kaedah yang salah hanya menghasilkan status 404 tidak ditemui. Status yang tidak dilaksanakan menunjukkan bahawa kaedah itu belum dilaksanakan "belum." Pencipta API boleh menggunakan status ini untuk memberitahu pelanggan bahawa kaedah ini akan tersedia untuk mereka pada masa hadapan.	
Different possible error messages. For example: *Unexpected SOAP message*	1. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Invalid content type: <*content type*>	1. Jenis kandungan mesej SOAP mestilah teks/xml, xop/xml, soap/xml atau *multipart/related*. 2. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]).	
Must use POST request method instead of	1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan SOAP menggunakan kaedah HTTP POST.	

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Unsupported HTTP *method*	1. Sistem maklumat pelanggan perkhidmatan mesti menghantar mesej permintaan REST menggunakan kaedah HTTP HEAD, GET, DELETE, POST, PUT atau PATCH.	
A number of different error messages depending on cause of the error. Contohnya, org.xml.sax.SAXParseException; *Premature end of file*.	1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP yang tidak betul. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Malformed SOAP message: *body missing*	1. Sistem maklumat pelanggan perkhidmatan menghantar mesej SOAP tanpa *body*. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]). 2. Untuk butiran lanjut tentang ralat, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Malformed SOAP message: *header missing*	1. Sistem klien perkhidmatan menghantar mesej SOAP tanpa *header*. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PRMESS]). 2. Untuk butiran lanjut tentang *error*, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	
Request does not have SOAP message	1. Sistem klien perkhidmatan menghantar *multipart* MIME *envelope* yang tidak mempunyai mesej SOAP sebagai komponen pertamanya. Pastikan mesej diformat dengan betul (untuk maklumat lanjut, lihat [UXP-PR-MESS]). 2. Untuk butiran lanjut tentang ralat, semak log proksi *Security Server* klien perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server).	

3.1.3 Ralat Daripada Security Server Agensi Pengguna

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Could not find addresses for service provider 'SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE'	1. Perkhidmatan ini tidak didaftarkan dalam *Security Server* pembekal perkhidmatan. Semak sama ada kod perkhidmatan dalam mesej permintaan adalah sama dengan kod yang didaftarkan dalam *Security Server* pembekal perkhidmatan.	
Client 'SUBSYSTEM:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT' not found	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Subsistem tidak didaftarkan dalam *Security Server* pelanggan perkhidmatan. Daftarkan subsistem (lihat Bahagian User Guide-Security Server Menambah Klien Pelayan Keselamatan)
A number of different error messages depending on cause of the error.	1. Terdapat pelbagai sebab yang berbeza. Semak log proksi untuk mendapatkan butiran lanjut (var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server)	
Token 'softToken' not active.	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Token perisian *Security Server* pelanggan perkhidmatan tidak dilog masuk. Masukkan PIN token perisian daripada *User Interface Security Server* pelanggan perkhidmatan.
Security server has no valid authentication certificate	1. Hubungi pentadbir *Security Server*	1. *Security Server* pelanggan perkhidmatan tidak

	pelanggan perkhidmatan	mempunyai sijil pengesahan yang sah. Pastikan semua syarat berikut dipenuhi: (i) *Security Server* mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk Pelayan Keselamatan) (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan). (iv) Sijil aktif (lihat Bahagian User Guide-Security Server

		Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil)
Service provider did not send correct authentication certificate	1. Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. *Security Server* pembekal perkhidmatan tidak mempunyai sijil pengesahan yang sah. Pastikan semua syarat berikut dipenuhi: (i) *Security Server* mempunyai sekurang-kurangnya satu sijil pengesahan (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Pengesahan dan Sijil untuk Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide-Security Server Ketersediaan Keadaan Token

		Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Bahagian User Guide-Security Server Pendaftaran Negeri Pengesahan dan Sijil Penyulitan). (iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian User Guide-Security Server Status Kesahan Sijil).
Client specifies HTTPS but did not supply TLS certificate	1. Sijil TLS sistem maklumat pelanggan perkhidmatan mesti dimuat naik ke *Security Server* pelanggan perkhidmatan (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).	
Could not find any certificates for member	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Subsistem pelanggan perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar: (i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh

		subsistem tersebut (lihat Bahagian User Guide-Security Server Mengkonfigurasi Kunci Tandatangan dan Sijil untuk Pelanggan Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian User Guide Security Server Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Negeri Pendaftaran Bahagian User Guide-Security *Server* bagi Sijil Menandatangani). (iv) Sijil aktif (lihat Bahagian User Guide-Security Server Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP sijil adalah baik (lihat Bahagian User Guide-Security Server

		Kesahan Negeri Sijil)
No space left on device	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. Pastikan *Security Server* pelanggan perkhidmatan mempunyai ruang cakera kosong. Jika cakera dipisahkan, pastikan *partition* yang berkaitan mempunyai ruang kosong
Cannot timestamp messages: no timestamping services configure	1. Hubungi pentadbir Security Server pelanggan perkhidmatan	1. Pastikan syarat berikut adalah benar: (i) *Security Server* pelanggan perkhidmatan boleh menyambung ke perkhidmatan *timestamp*. Semak bahawa semua *firewall* api dikonfigurasikan dengan betul. (ii) Perkhidmatan *timestamp* tersedia. Semak log proksi (/var/log/uxp/proxy.log) untuk butiran lanjut
Global configuration is expired	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. *Security Server* klien perkhidmatan tidak boleh memuat turun konfigurasi global daripada pelayan pendaftaran. Semak log klien konfigurasi (/var/log/uxp/configuration_client.log) untuk butiran

Could not connect to target host (https://:5500)	1. Hubungi pentadbir *Security Server* pelanggan perkhidmatan	1. *Security Server* pelanggan perkhidmatan tidak boleh menyambung ke *Security Server* pembekal perkhidmatan. Pastikan firewall dikonfigurasikan dengan betul pada kedua-dua belah pihak: *Security Server* pelanggan perkhidmatan mesti membenarkan trafik keluar ke port *Security Server* penyedia perkhidmatan 5500 dan 5577, *Security Server* penyedia perkhidmatan mesti membenarkan trafik masuk ke port 5500 dan 5577.
Name or service not known. No address associated with hostname.	1. Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. *Security Server* pembekal perkhidmatan tidak dapat ditemui kerana *Security Server* didaftarkan dengan FQDN yang salah.

3.1.4 Ralat Daripada Security Server Agensi Pembekal

Mesej Ralat	**Penyelesaian Pentadbir Perkhidmatan**	**Penyelesaian Pentadbir *Security Server***
Request is not allowed: SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EX	*Security Server* pembekal perkhidmatan mesti memberikan hak akses kepada perkhidmatan dan kepada subsistem pelanggan perkhidmatan. Lihat Hak Akses Bahagian	

AMPLE_DEPARTMENT/EXAMPLE_SERVICE		
Malformed SOAP message: header missing	Sistem maklumat pembekal perkhidmatan mesti mengembalikan semua pengepala UXP yang wajib. Lihat [UXP-PR-MESS] untuk butiran lanjut.	
A number of different error messages depending on cause of the error. For example, org.xml.sax.SAXParseException; Premature end of file.	Sistem maklumat pembekal perkhidmatan mengembalikan mesej SOAP yang tidak betul. Untuk butiran lanjut tentang error, semak log proksi *Security Server* penyedia perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam User Interface Security Server)	
Unknown service: SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE	Pastikan kod perkhidmatan dalam mesej permintaan sepadan dengan perkhidmatan di bahagian pembekal perkhidmatan.	
The reason the connection failed. For example, Server responded with error 403: Forbidden	1. Pastikan *Security Server* pembekal perkhidmatan dibenarkan untuk menyambung ke sistem maklumat pembekal perkhidmatan dan sambungan dikonfigurasikan dengan betul. 2. Untuk maklumat lanjut tentang mengkonfigurasi sambungan, lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan. Untuk butiran lanjut tentang ralat, lihat log proksi *Security Server* pembekal perkhidmatan (/var/log/uxp/proxy.log atau daripada Log dalam *User Interface Security Server*.	
Server certificate is not trusted	Pilihan "Sahkan sijil TLS" dipilih dalam konfigurasi perkhidmatan, tetapi sijil sistem maklumat pembekal perkhidmatan belum dimuat naik ke *Security Server* penyedia perkhidmatan. Muat naik sijil sistem maklumat pembekal perkhidmatan ke *Security Server* (lihat Bahagian Komunikasi dengan Sistem Maklumat Pelanggan).	
Could not find any certificates for member 'SUBSYSTEM:SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT'	1. Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. Subsistem pembekal perkhidmatan tidak mempunyai sijil tandatangan yang sah. Pastikan syarat berikut adalah benar: (i) Terdapat sekurang-kurangnya satu sijil tandatangan untuk ahli yang dimiliki oleh

		subsistem tersebut (lihat Bahagian User Guide *Security Server* - Mengkonfigurasi Kunci Tandatangan dan Sijil untuk Pelanggan Pelayan Keselamatan). (ii) Sijil adalah pada token yang dilog masuk dan tersedia (lihat Bahagian *User Guide Security Server* Ketersediaan Keadaan Token Keselamatan, Kunci dan Sijil). (iii) Sijil didaftarkan (lihat Negeri Pendaftaran Bahagian *User Guide-Security Server* bagi Sijil Menandatangani) (iv) Sijil aktif (lihat Bahagian *User Guide-Security Server* Mengaktifkan dan Melumpuhkan Sijil). (v) Sambutan OCSP bagi sijil adalah baik (lihat Bahagian *User Guide-Security Server* Status Kesahan Sijil).
Connection pool shut down	Hubungi pentadbir *Security Server* pembekal perkhidmatan	*Security Server* pembekal perkhidmatan tidak boleh mengakses pangkalan datanya. Semak log proksi (/var/log/uxp/proxy.l og) dan log Postgres (/var/log/postgresql/) untuk butiran lanjut
Failed to get signing info for member HttpError: Connection to Signer (port 5558) timed out	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Cuba mulakan semula proses penandatangan $ systemctl mulakan semula uxp-signer. Semak log penandatangan var/log/uxp/signer.log untuk mendapatkan maklumat lanjut.

Token 'softToken' not active	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Pastikan bahawa token perisian *Security Server* pembekal perkhidmatan telah dilog masuk. Jika ia tidak dilog masuk, log masuk daripada *Security Server User Interface* pembekal perkhidmatan.
Cannot timestamp messages: no timestamping services configured	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Anda mesti mengkonfigurasi perkhidmatan timestamp untuk *Security Server* pembekal perkhidmatan (lihat Bahagian *User Guide- Security Server* Mengurus Perkhidmatan Timestamp).
Cannot timestamp messages	Hubungi pentadbir *Security Server* pembekal perkhidmatan	1. Walaupun terdapat perkhidmatan *timestamp* yang dikonfigurasikan (lihat mesej ralat sebelumnya),*timestamp* masih boleh gagal. Masalah berikut mungkin berlaku: (i) Terdapat masalah pada bahagian perkhidmatan timetamp dan perkhidmatan tidak tersedia. Semak log proksi (var/log/uxp/proxy .log) untuk butiran lanjut. (ii) *Security Server* pembekal perkhidmatan tidak boleh menyambung ke perkhidmatan timestamp. Pastikan bahawa firewall dan port dikonfigurasikan dengan betul untuk kedua-dua perkhidmatan *Security Server* dan *timestamp*.
Global configuration is expired	Hubungi pentadbir *Security Server* pembekal perkhidmatan	Cuba mulakan semula proses klien konfigurasi $ systemctl mulakan semula uxp-confclient. Ada kemungkinan

		Security Server penyedia perkhidmatan tidak dapat menyambung ke pelayan pendaftaran untuk memuat turun konfigurasi global. Pastikan konfigurasi *firewall* api di kedua-dua belah adalah betul. Lihat log klien konfigurasi untuk butiran lanjut (/var/log/uxp/configuration_client.log)

JABATAN PEMBANGUNAN KEMAHIRAN
KEMENTERIAN SUMBER MANUSIA

INTERFACE DESCRIPTION DOCUMENT (IDD)
PEMBANGUNAN API - <NAMA AGENSI>

DATA RAYA TVET

Disediakan oleh:
<Nama Agensi Pembekal><versi>

Tarikh Disediakan:
Xx/xx/202x

SEMAKAN DAN PENGESAHAN DOKUMEN

Dokumen ini disedia dan disemak oleh pasukan projek pembangun sistem

Disemak Oleh	Jawatan	Tandatangan	Tarikh Semakan

Dokumen ini disahkan oleh pemilik bisnes dan sistem yang akan dibangunkan.

Disahkan Oleh	Jawatan	Tandatangan	Tarikh Semakan

KAWALAN DOKUMEN

No. Versi	Tarikh	Ringkasan Pindaan	Penyedia

KANDUNGAN

TAJUK **MUKA SURAT**

No Rujukan Fail			
Nama Projek	Projek Menaik Taraf Sistem Pengurusan Integrasi Kemahiran Malaysia (MySPIKE) Ke Arah Data Raya TVET		
Nama Modul	Pembangunan API Data Raya TVET - <NAMA AGENSI>		
Pengurus Projek	Unit Pengurusan Maklumat		
SME Modul	Unit Pengurusan Maklumat		
Pemilik Projek	Jabatan Pembangunan Kemahiran		
Tarikh Mula		**Tarikh Selesai**	

1 OBJEKTIF

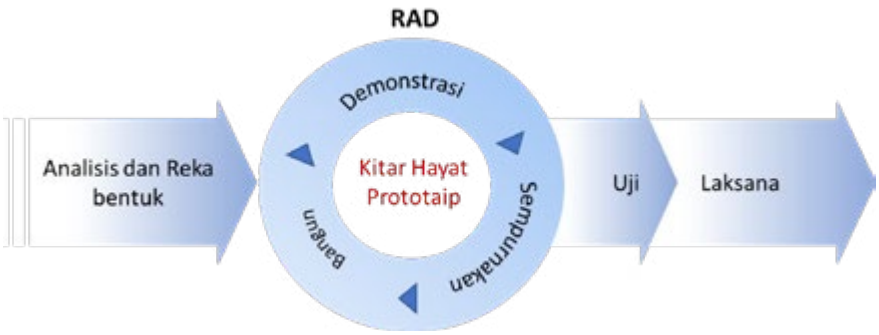
i. Penyediaan Struktur Data
ii. Pembangunan API
iii. Pengujian
iv. Pelaksanaan

2 PENDEKATAN PEMBANGUNAN

Pelaksanaan projek dibangunkan secara dalaman (*in-house*) oleh Pasukan Unit Pengurusan Maklumat (UPM), Jabatan Pembangunan Kemahiran (JPK), Kementerian Sumber Manusia(KESUMA).

Bil	Jenis Data	Kaedah Pemadanan Data
1.	Pendaftaran pelajar	API
2.	Persijilan pelajar	API
3.	Pengajar	API
4.	Permohonan	API

3 MODEL PROSES



Rajah 1 : Metodologi RAD

Putaran ***Rapid Application Development*** (RAD) digunapakai dalam membangunkan MySPIKE. RAD merangkumi 4 fasa utama iaitu perancangan keperluan, reka bentuk, pembangunan dan pelaksanaan. Fasa ini dilaksanakan oleh sekumpulan pembangun aplikasi yang mahir yang bekerjasama rapat dengan pengguna sepanjang tempoh pembangunan. Teknik dan tools yang digunakan merupakan faktor utama kejayaan RAD. Matlamat utama metodologi ini adalah menghasilkan sistem yang berkualiti tinggi secara cepat dengan memberikan penekanan terhadap keperluan pengguna.

4 API

A. DATA PENDAFTARAN PELAJAR

i. Url : https://

ii. Methods : POST / GET

iii. Data Types : JSON / Raw

iv. Request :

Authorization: Bearer Token / API Key / Basic Auth

Bil	Return Data	Data Type	Required

v. Response

Bil	Parameter	Data Type	Required	Sample Data
1.	success	string		true
2.	data	array		[…]
3.	message	string		Data accepted

B. DATA PERSIJILAN PELAJAR

i. Url : https://

ii. Methods : POST / GET

iii. Data Types : JSON / Raw

iv. Request :

Authorization: Bearer Token / API Key / Basic Auth

Bil	Return Data	Data Type	Required

v. Response

Bil	Parameter	Data Type	Required	Sample Data
1.	success	string		true
2.	data	array		[…]
3.	message	string		Data accepted

C. DATA PENGAJAR

i. Url : https://

ii. Methods : POST / GET

iii. Data Types : JSON / Raw

iv. Request :
Authorization: Bearer Token / API Key / Basic Auth

Bil	Return Data	Data Type	Required

v. Response

Bil	Parameter	Data Type	Required	Sample Data
1.	success	string		true
2.	data	array		[…]
3.	message	string		Data accepted

D. LOGIN UP_TVET

i. Url : https://

ii. Methods : POST / GET

iii. Data Types : JSON / Raw

iv. Request :

Authorization: Bearer Token / API Key / Basic Auth

Bil	Parameter	Data Type	Required
1.	no_ic	String	Yes
2.	password	String	Yes

v. Response

Bil	Parameter	Data Type	Required	Sample Data
1.	success	string		true
2.	data	array		[…]
3.	message	string		Data accepted

E. PERMOHONAN UP_TVET

i. Url : https://

ii. Methods : POST / GET

iii. Data Types : JSON / Raw

iv. Request :

Authorization: Bearer Token / API Key / Basic Auth

Bil	Return Data	Data Type	Required
1.	…	String	Yes

v. Response

Bil	Parameter	Data Type	Required	Sample Data
1.	success	string		true
2.	data	array		[…]
3.	message	string		Data accepted

5 KESIMPULAN

Dokumen ini adalah rujukan pembangunan API bagi integrasi antara sistem milik agensi dan Data Raya TVET. Pembangunan API ini telah membolehkan sistem Data Raya TVET mengumpul maklumat pendaftaran, persijilan dan pengajar dan agensi mengumpul maklumat permohonan UP_TVET.

LAMPIRAN

Jadual Rujukan (table Reference)

KEMENTERIAN SUMBER MANUSIA

JABATAN PEMBANGUNAN KEMAHIRAN

Tingkat 7- 8, Setia Perkasa 4,
Kompleks Setia Perkasa,
Pusat Pentadbiran Kerajaan Persekutuan,
62530 Putrajaya

No. Telefon : 03-8886 5589

https://www.dsd.gov.my
https://www.tvet.gov.my