**STAGE 1 – VALUE ADDED RESELLING**

**DATA ACCESS SUB-LICENCE**

**APPLICATION**

## Applicant Details

|  |  |
| --- | --- |
| **Date of Application:** | [●] |
| **Name of the Licence Applicant:** | [●] (the **Applicant**) |
| **Registered Address:**  | [●] |
| **ABN/ACN:** | [●] |
| **Is the Applicant a "foreign person" within the meaning of the Foreign Acquisitions and Takeovers Act 1975 (Cth)?** | [Yes/No] [Details] |
| **Applicant Contact Person:** | [●] |
| **Contact Address:** | [●] |
| **Telephone:**  | [●] |
| **Mobile:**  | [●] |
| **Fax:**  | [●] |
| **Contact Email for signatory:**  | [●] |

The signatory hereby declares that the signatory is authorised to apply for a licence on behalf of the Applicant, and that the information contained in this completed Application Form is true and correct.

|  |  |  |
| --- | --- | --- |
| **Executed** by [Insert Applicant Name and ABN/ACN]by its authorised signatory: |  |  |
| Authorised Signatory |  |  |
|  |  |  |
| Name of Authorised Signatory(BLOCK LETTERS) |  | Position / Title of Authorised Signatory |

**INSTRUCTIONS**

**Do not send supporting information or documentation with this Application, other than where specifically identified.**

*Any reference to the “Principal” below, is to be read as a reference to Land Services SA Operating Pty Ltd ACN 618 229 815 as trustee for the Land Services SA Operating Trust ABN 86 836 650 939 in its capacity as the State's appointed service provider.*

Once you have completed the Stage 1 Application Form in its entirety please send via email to *DataAccess@landservices.com.au****.*** If you do not receive an email acknowledgment within 2 Business Days please contact LSSA’s Customer Service on (08) 8423 5000 or email customersupport@landservices.com.au.

*In order to become a Value Added Reseller (****VAR****) Licensee, the Applicant must meet the* ***Mandatory Criteria*** *set out below or as required by the State of South Australia (****State****), from time to time.*

*The Applicant must provide sufficient responses in this Application to enable the Principal to assess the Application in respect of all of the below* ***Mandatory Criteria****.*

*A "Yes" response which includes comments such as “subject to conditions”, or which details any other conditions for any of the* ***Mandatory Criteria****,**may be treated as a "No" response if those conditions are not acceptable to the Principal.*

*The Application will be assessed by the Principal, however the State will have the absolute discretion whether to approve or reject the Application. The Applicant will be required to provide evidence to show that it meets the Mandatory Criteria (including proof that the Applicant has passed a technical data security audit and evidence of its privacy and insurance arrangements), in order to enable the appropriate assessment of the Application and the proposed products. The State may take into consideration any relevant matters, such as National Security, in its decision whether to approve or reject the application.*

*If the Application does not meet the Mandatory Criteria as demonstrated by the responses set out in this Application, the Applicant will be notified by the Principal, informed of the reasons why the Application has been rejected, and advised of the Applicant's rights of appeal.*

**MANDATORY CRITERIA**

1. The Applicant intends to use the data for a commercial purpose;
2. The Applicant will abide by the terms and conditions of the Data Access Sub-Licence Agreement. This includes the Applicant providing its explicit agreement to:
	* 1. pay a licence fee to the Service Provider in accordance with the terms of the Data Access Sub-Licence Agreement; and
		2. abide by any restrictions on the removal, transmission or transfer of the State's data outside of Australia as required by the terms of the Data Access Sub-Licence Agreement;
3. The Applicant can demonstrate that it has appropriate data security arrangements in place;
4. The Applicant can pass a technical data security audit and agrees to submit to regular technical data security audits;
5. The Applicant has downstream control of data to end users that satisfies the Principal’s requirements and the State’s mandatory minimum specifications;
6. The Applicant's privacy plans, policies and practices meet the requirements of the Australian Privacy Principles as set out in the *Privacy Act 1988* (Cth);
7. The Applicant is financially viable;
8. The Applicant has appropriate insurance in place;
9. The Applicant is reputable, in that the Applicant is capable of adequately planning and managing development and delivery of product to market;
10. The Applicant has adequate internal quality assurance processes in place;
11. The Applicant's Application can be confirmed through referee reports (by way of provision of three references).
12. **INTENDED USE OF THE DATA**
	1. **Does the Applicant intend to use the data for a commercial purpose?**

Please indicate your answer below by clearly indicating your chosen response.

*If yes, please summarise the intended use in the comments.*

*If no, contact the Principal to discuss next steps - DO NOT COMPLETE THIS APPLICATION*

**RESPONSE:**

**o YES**

**o NO**

***Comments (optional):***

* 1. **Scope of data required by the Applicant.**

Please indicate your answer below by clearly indicating your chosen response.

|  |  |
| --- | --- |
| **Scope of Data** | [Whole of State of South Australia] / [The following Local Government Area(s): [●]; [●].] |
| **Delivery Frequency** | [Daily Data Extract / Weekly Data Extract]. The Daily Data Extract incurs an additional fee of $[●]. |

1. **DATA ACCESS SUB-LICENCE AGREEMENT**
	1. **If the Applicant is granted a licence, the Applicant agrees to:**
	2. **fully accept all of the terms and conditions of the Data Access Sub-Licence Agreement;**
	3. **pay any nominated licence fees, in accordance with the Data Access Sub-Licence Agreement terms and conditions;**
	4. **submit to technical data security audits to be performed as required under the Data Access Sub-Licence Agreement terms and conditions;[[1]](#footnote-2)**
	5. **comply with the Data Access Sub-Licence terms and conditions regarding any restrictions on the removal, transmission or transfer of the data outside of Australia.**

The Principal requires each licensee to accept and agree to be bound by the same terms and conditions of use, as detailed in the Data Access Sub-Licence Agreement.

Please indicate your answer below by clearly indicating your chosen response.

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

1. **DATA SECURITY ARRANGEMENTS**

**Based on the responses to sections 3.1, 3.2 and 3.3, LSSA will review the responses and the Applicant may be required to complete an Additional High Risk Security Assessment. The Principal will send a copy of this assessment once this application has been completed and submitted to the Principal.**

* 1. **Initial Data Security Assessment**

Applicants are required to provide details of the data security arrangements that currently exist (or will be implemented) to protect licensed data from unauthorised access and to ensure that it is not used in a manner contrary to the terms of the Data Access Sub-Licence Agreement.

Please clearly indicate if any of the below are proposed arrangements (i.e. they do not currently exist).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| * 1. **Organisational Context**

|  |
| --- |
| **Please give an overview of the Applicant’s organisation and its purpose?** |
|  |

* 1. **Data Usage**

*This question is posed to identify if in anyway the Wholesale Sales Data will be linked with other datasets, and from that Personal Information (****PI****) could possibly be generated. Such as matching addresses to names, phone numbers, emails, etc. For more information about what is consider PI please visit this link* [*https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information*](https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information)*.*

|  |
| --- |
| **Will the Wholesale Sales Data provided by the Principal through the VAR license be combined with other datasets? (Yes/ No)**  |
|  |
| **If Yes,** | What data is contained within these separate datasets that will be combined?  |
|  |
| **If No,**  | Are there future plans to do so? |
|  |

* 1. **Data Storage**

|  |
| --- |
| **Please confirm that the Wholesale Sales Data provided by the Principal to the Applicant will be stored exclusively within Australia?** |
|  |

|  |
| --- |
| **Will the Wholesale Sales Data be stored within a Cloud service? (Yes/No)** |
|  |
| **If Yes,** | What cloud provider and service will be used to store the Wholesale Sales Data? |
|  |

* 1. **Access Control to Data**

|  |
| --- |
| **Will the Applicant restrict access to Wholesale Sales Data to only appropriate members within the organisation? (Yes/ No)** |
|  |
| **If Yes,** | How will the Applicant restrict access and what members will be given access?  |
|  |
| **If No,** | Please explain how and why? |
|  |
| **Will the relevant controls and the access for these members be periodically reviewed? (Yes/ No) (If yes, please detail frequency).** |
|  |

* 1. **Overseas Customers/Users**

|  |
| --- |
| **Will the Principal data be accessible to out-sourced services used by the Applicant’s organisation? (Yes/ No)** |
|  |
| **Does your organisation have customers/users that are overseas?** |
|  |

 |

* 1. **Certification to Security Standards**

Please identify and provide evidence if your organisation has been assessed against or is certified to any of the following standards:

**CERTIFICATION:**

**o ISO 27001**

**o SOC2**

**o ISAE 3402**

|  |
| --- |
| **Comments (optional):** |
| [●] |

NOTE: If the Applicant has identified that they are currently certified or have been assessed against one of the above standards, and can provide satisfactory evidence of this to the Principal, then the Applicant will NOT be required to complete Section 3.3. Security Self-Assessment Questionnaire.

* 1. **Security Self-Assessment Questionnaire**

**For Applicants that do not currently have a certification or has not been independently assessed against the above standards (or cannot satisfactorily provide evidence of, are required to complete the following Self-Assessment Questionnaire). This Section 3.3 questionnaire is for the Applicant to provide details on their cyber security capabilities that are currently in place.**

**Depending on the results of the Security Self-Assessment Questionnaire, as assessed by the Principal, you may be asked to complete an Additional High Risk Security Assessment (which will be provided by the Principal as required).**

**Instructions for Applicant: Please indicate 'X' against the single most applicable option for each question. Provide further information, justification, or context in the Justification column.**

**Where appropriate, please provide documentation or evidence to support statements.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question** | **Tier 1** | **x** | **Tier 2** | **x** | **Tier 3** | **x** | **Justification** |
| **Does your organisation have a risk management program, and do you have a good understanding of the security risks you face?** | There is no formal program in place, we have a limited understanding of the cyber threat landscape and risks to our organisation, and no defined process to help reduce the likelihood of being successfully attacked.  |   | We have a general understanding of the cyber threat landscape and risks to our organisation, additionally we have a risk register that covers cyber security risks but not updated regularly.  |   | We undertake regular risk assessments of our business and identify any cyber security risk and their relative importance to our organisation. We also have formal processes in place to formally manage those risks and steps to take to improve our ability of handling them.  |   |   |
| **Does your organisation use access controls to appropriately restrict access to systems and networks?** | No access control measures or documentations is in place. |   | We have some access controls in place on critical systems within the organisation. Restricting access based on if the user is privileged or unprivileged. |   | We have documented policy and processes (e.g., System Usage Policy, Access Request Policy) for organisation wide access control. Restricting access based on business use.Role-Based Access Control (RBAC) or similar is used by the organisation to define access. |   |   |
| **Does your organisation use authentication controls such as Multi-Factor Authentication (MFA) to prevent unauthorised access to systems, networks, and data?** | No authentication controls such as MFA is in place. |   | We have MFA controls across some of our critical systems/applications. The authentications are not centrally monitored or logged. |   | We have MFA controls across all systems and applications to authenticate both unprivileged and privileged users, and successful and unsuccessful authentication events are centrally logged and monitored by staff. MFA policy and processes are documented and regularly reviewed. |   |   |
| **Does your organisation have specific processes for importing and exporting data, to protect data in transit internally and externally?** | We do not have any data transfer processes or procedures are in place. |   | We have a documented policy and process, providing high level guidance on data transfer procedures. |   | We have documented policy and processes regarding data transfers and controls in place to restrict, monitor and log transferred data internally and externally.Data transfer logs are also verified on a regular basis. |   |   |
| **Question** | **Tier 1** | **x** | **Tier 2** | **x** | **Tier 3** | **x** | **Justification** |
| **Does your organisation use end user device hardening controls (e.g., Application Allow Lists, Executable Blocking) across systems and networks?** | No End User Device Hardening controls are in place. |   | We have documented policy and process for End User Device Hardening, which includes password complexity requirements on devices. |   | We have well-documented policy and processes for End User Device Hardening. Covering application block/allow lists, password complexity, duration and lock out requirements, and automatic patching. |   |   |
| **Does your organisation perform independent security assurance activities, such as penetration testing?** | We do not perform any independent security assurance activities currently. |   | We have had security assurance activities completed in the past such as a penetration test, but not on a frequent or scheduled basis. |   | We have a documented security calendar to regularly schedule security assurance practices that are completed and addressed in a timely manner. Contracting trusted independent third parties to perform in-depth penetration testing across all internal and external systems. |   |   |
| **Does your organisation have a patching and vulnerability management program?** | We do not have any patching and vulnerability management practices in place. |   | We have a documented policy and process regarding patching organisation systems. And have performed vulnerability management practices in the past but not on a regular or scheduled basis. |   | We have a documented policy and process for both Patching and Vulnerability management which are performed on a frequent and regular basis. Covering all organisation systems, networks, applications, and devices. Patching and remediating vulnerabilities is completed in a timely manner and based on criticality. |   |   |
| **How does your organisation respond and manage security incidents?** | We do not have an incident response plan or formal procedures in place.  |   | We have a documented policy and process, providing high level response activities and guidance on who to engage and communicate with when an incident occurs.  |   | We have documented policy and processes (e.g., Data Breach Notification Policy, Incident Response Plan) and security incidents are recorded and, where appropriate, allocated an owner to manage the incidents. Plans and processes are reviewed and tested regularly. We engage and communicate with key stakeholders and customers in response to an incident.  |   |  |
| **Question** | **Tier 1** | **x** | **Tier 2** | **x** | **Tier 3** | **x** | **Justification** |
| **Does your organisation have measures in place to monitor and record any security events on your key systems or networks and** **ensure that the proper people are notified of an incident?**  | No logging in place, or some logging is in place but this is not reviewed. |   | We have documented processes to notify appropriate stakeholders and third parties of security incidents. But have limited logging in place that record security events but don't capture everything. We use these logs for investigation purposes only. |   | We have a well-documented policy and procedure for notifying appropriate stakeholder, third parties and Government Security organisations (e.g. ASD) of security incidents that are occurring as soon as identified.And have a logging and monitoring solution in place which records relevant security events that occur on our key systems and devices. These are monitored on an ongoing basis either by someone internally or an external provider. |   |  |
| **Does your organisation have processes and technologies in place to recover the operation of your critical systems which may be affected by a security incident?**  | We have limited business continuity and resilience for our critical systems and have no testing. |   | We have documented business continuity and disaster recovery plans in place. These are not tested regularly.Some backups are retained, but we do not regularly test them, and they have not been designed using a risk-based approach. |   | We have documented business continuity and disaster recovery plans. These are regularly reviewed and tested at least annually.A risk-based backup architecture is in place for critical systems, and regular testing of backups occurs. |   |   |
| **Does your organisation undertake pre-employment background screening of staff to determine if they present a security risk to your organisation?** | We don’t do any screening of our employees prior to, or during employment. |  | No formal process is in place, but generally we perform pre-employment background checks of staff prior to onboarding. |  | Formal process in place requiring pre-employment checks occur, and where appropriate we require staff to undertake background checks throughout their employment. |  |  |
| **Declaration**  |   |   |
| *The above responses to the questions are a true and correct reflection of the security posture of the organisation.*  |

1. **PRIVACY**

**Although the licensed data does not contain names of natural persons, it is a licence condition that sub-licensees do not diminish the privacy of natural persons by any means, including data matching or correlating the licensed data with data from other sources.**

**Applicants are accordingly required to demonstrate that their privacy plans, policies and practices meet the requirements of the Australian Privacy Principles to protect licensed data from unauthorised access and to ensure that personal information contained in licensed data is not used in a manner contrary to the *Privacy Act 1988* (Cth), the terms of the Data Access Sub-Licence Agreement or the Information Privacy Principles.**

*Note: A copy of the Applicants privacy plan and policy will need to be provided with this Application before the State will approve the execution of a Data Access Sub-Licence Agreement.*

* 1. **Privacy Framework**

Do the Applicant's privacy plans, policies and practices comply with the requirements of the Australian Privacy Principles?

**RESPONSE**:

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Privacy Breach**

Has the Applicant been involved in any claim or dispute associated with breaches of privacy?

*If yes, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

1. **FINANCIAL VIABILITY**

**Applicants are required to demonstrate that they have the financial capacity to perform all obligations required by the licensing arrangements (as detailed in the Data Access Sub-Licence Agreement).**

**This includes the Applicant providing its permission for the Principal to perform due diligence enquiries on the Applicant that may include financial, credit and security checks and a background search with prudential regulatory authorities.**

**Your responses below will be assessed against the Principal's mandatory minimum specifications, a copy of which can be obtained upon request.**

* 1. **Bankruptcy**

Are there or have there been any bankruptcy actions against a director of the Applicant, its parent or any associated entity within the past 5 years?

*If yes, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Insolvency**

Are there or have there been any actions of insolvency proceedings, actual or threatened (including Voluntary Administration or Application to Wind Up) against the Applicant, its parent or any associated entity within the past 5 years?

*If yes, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **De-registration actions**

Are there or have there been any de-registration actions against the Applicant, its parent or any associated entity within the past 5 years?

*If yes, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Solvency**

Is the Applicant trading solvent, and able to meet its debts as and when they fall due in the normal course of business?

*If no, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Third party checks**

Does the Applicant give permission for the Principal to make due diligence enquiries and perform financial, credit, security and background checks as deemed appropriate by the Principal?

*If no, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

1. **INSURANCE**

**The Principal requires each sub-licensee to maintain adequate public liability and professional indemnity insurances for the entire term of the Data Access Sub-Licence Agreement.**

**Successful Applicants are required to provide copies of certificates of insurances (in the name of the Applicant entity) in the amounts of $20 million AUD for public liability and professional indemnity of $5 million AUD (for any one claim) and $10 million AUD (in aggregate claims).**

**Applicants who do not currently have sufficient insurance cover must state their preparedness (below) to acquire such insurance cover in the event a provisional grant of a licence to that Applicant is subsequently made.**

*Note: Evidence of adequate insurance will be required before a Data Access Sub-Licence Agreement will be executed.**If available, the Applicant should enclose with this Application a certificate of currency in relation to the Insurance Arrangements referred to at (a) below.*

* 1. **Insurance levels**

Does the Applicant's current insurance satisfy this requirement?

*If yes, please provide details of the insurer, level of cover and type of cover.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Insurance Commitment**

Does the Applicant agree to have insurance that satisfies this requirement before a Data Access Sub-Licence Agreement is executed?

*If no, please provide details in the comments.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

1. **EXPERIENCE**

**Since execution of a Data Access Sub-Licence Agreement between a successful Applicant and the Principal will establish an on-going commercial relationship between the parties for the term of the Data Access Sub-Licence Agreement, it is a requirement of the Principal that the Applicant is able to demonstrate historical sound corporate behaviour, and an ability to research, plan, develop and deliver new information products.**

*Note: The Principal will treat all information provided by the Applicant as commercial-in-confidence.*

*If the Applicant's experience includes:*

* *utilising services of third parties to develop and/or support delivery of the Applicant's information products/services; and/or*
* *servicing markets outside of Australia,*

*separate supporting details of those arrangements must be supplied (e.g.: nature and extent of the arrangements) to the State.*

* 1. **Experience in information services market**

Does the Applicant have any experience in the information services market and/or the value-adding of data?

*Please indicate in the comments if this experience includes servicing markets outside of Australia.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Experience in development of land information products**

Does the Applicant have any experience in the development and delivery of property and land information products?

*Please indicate in the comments if this experience includes servicing markets outside of Australia.*

**RESPONSE:**

|  |  |
| --- | --- |
| **□** | **Yes** |
| **□** | **No** |
| **Comments (optional):** |
| [●] |

* 1. **Organisation history**

Please provide a brief history of the Applicant to demonstrate the Applicant organisation’s stability and maturity.

|  |
| --- |
|  |

1. **QUALITY ASSURANCE PROCESSES**

**Quality assurance processes assist organisations to mitigate risk and to satisfy compliance requirements.**

**Please provide details of the Applicant's corporate quality assurance processes including details of any Quality Management Systems used in respect of data management.**

|  |
| --- |
|  |

1. **REFEREE REPORTS**

**The Applicant is to provide a maximum of three (3) referees that are willing to respond to enquiries made by the Principal in relation to this Application.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Details** | **Reference 1** | **Reference 2** | **Reference 3** |
| *Referee organisation name:* |  |  |  |
| *Referee organisation address:* |  |  |  |
| *Nature of relationship between the Applicant and the Referee:* |  |  |  |
| *Period of association between the Applicant and the Referee:* |  |  |  |
| *Referee contact person name:* |  |  |  |
| *Referee contact person phone number:* |  |  |  |
| *Referee contact person email address:* |  |  |  |

1. Data security audits will be used to assess applications used by the licensee that supply data to customers and to assess the infrastructure supporting those applications. [↑](#footnote-ref-2)