**LICENSEE SELF-ASSESSMENT COMPLIANCE STATEMENT**

Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Licensee name:** |  | | | |
| **ABN / ACN:** |  | | | |
| **Data Access Sub-Licence Agreement** | Dated Click or tap to enter a date. between the Licensee and Land Services SA Operating Pty Ltd as trustee for the Land Services SA Operating Trust (**LSSA**) (**Data Access Sub-Licence Agreement**). | | | |
| **Compliance Period** | **Commencement** |  | **Expiry** |  |
| **List of Derivative Products (clause 9.1(b))** | For a complete list of all Derivative Products which are integrated with the Data and allow users to enquire upon the Data please see Annexure A. | | | |
| **Security Audit Report:[[1]](#footnote-2)** | [ Click or tap to enter a date. ] / [Not Applicable] | | | |
| **Security Audit Report** | The Licensee's progress in implementing each recommendation set out in the Security Audit Report is set out in Annexure B. | | | |

To the best of my knowledge, I certify the responses provided in, and attached to, this Self-Assessment Compliance Statement (**Compliance Statement**) are true and correct in all respects.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| **NAME** |  | **POSITION TITLE** |  | **SIGNATURE** |  | **DATE** |

**INSTRUCTIONS**

Once you have completed the LICENSEE SELF-ASSESSMENT COMPLIANCE Statement in its entirety please send via email to [*DataAccess@landservices.com.au*](mailto:DataAccess@landservices.com.au)***.*** If you do not receive an email acknowledgment within 2 Business Days please contact Customer Service on (08) 8423 5000 or email [customersupport@landservices.com.au](mailto:customersupport@landservices.com.au)

*To continue being a Value Added Reseller (****VAR****) Licensee, the Applicant must complete the Questionnaire set out below or as required by the State of South Australia (****State****), from time to time.*

*The Attestation will be assessed by the Principal, however the State will have the absolute discretion whether to approve or reject the Attestation.*

**QUESTIONNAIRE**

1. **GENERAL QUESTIONS**
   1. **VAR Licence**

|  |
| --- |
| **Does the organisation wish to continue having access to the Wholesale Sales Data Value Added Reseller (VAR) Licence given by LSSA? (Yes/ No)** |
|  |

* 1. **Organisational Context**

|  |  |
| --- | --- |
| **Has your organisation changed in any form? (People/Purpose/Location/Services) (Yes/ No)** | |
|  | |
| **If Yes,** | Please explain how it has changed? | |
|  | |

* 1. **Data Usage**

|  |  |
| --- | --- |
| **Has the position of this organisation combining Wholesale Sales Data with other datasets changed? (Yes/ No)** | |
|  | |
| **If Yes,** | Please explain how it has changed? |
|  |
| **If No,** | **(And is continuing to combine data)** Have any new external datasets been combined with the Wholesale Sales Data since last stated? |
|  |

* 1. **Data Security Controls**

|  |  |
| --- | --- |
| **Have any Data Security Controls as specified in the *Self-Assessment Questionnaire* or your original Application been changed, added, or removed from the organisation? (Yes/ No)** | |
|  | |
| **If Changed,** | How have specific controls been changed? |
|  |
| **If Added,** | What new controls have been added? |
|  |
| **If Removed,** | What specific controls have been removed and why? |
|  |

* 1. **Certifications**

|  |
| --- |
| **Has the organisation gained, or lost any information security certification or has been assessed against the following (ISO27001, SOC2, ISAE 3402)? (Yes/ No) If so, please detail which?** |
|  |

* 1. **Financial Viability and Insurance**

|  |  |
| --- | --- |
| **Has your organisation’s financial or insurance situation changed since last informing LSSA? (Yes/ No)** | |
|  | |
| **If Yes,** | Please explain how it has changed? |
|  |

1. **PRIVACY**
   1. **Has the Licensee been involved in any claim or dispute associated with breaches of privacy since last informing LSSA?**

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

**RESPONSE:**

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

1. **COMPLIANCE WITH DATA ACCESS SUB-LICENCE AGREEMENT (General)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Criteria** | **Clause No.** | **Summary of relevant Licence Condition** | **Licensee has fully complied with this requirement (Yes / No)** | **Details of any non-complying aspects and proposed remedies** |
|  | DATA ACCESS SUB-LICENCE AGREEMENT | - | The Licensee confirms that, except to the extent disclosed in this Statement, it has complied with the Data Access Sub-Licence Agreement in all respects. | Choose an item |  |

1. **COMPLIANCE WITH DATA ACCESS SUB-LICENCE AGREEMENT (Specific)**

Without limiting the above, the Licensee provides the following information on its compliance with the Data Access Sub-Licence Agreement:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Criteria** | **Clause No.** | **Summary of relevant Licence Condition** | **Licensee has fully complied with this requirement (Yes / No)** | **Details of any non-complying aspects and proposed remedies** |
|  | PRODUCT LICENCE | 3.2(a) | The Licensee may permit a person to use a Derivative Product only if that person has entered into a licence agreement with the Licensee that complies with the requirements of the Data Access Sub-Licence Agreement (**Product Licence**), and that Product Licence has not expired or otherwise terminated.  The Licensee confirms it has all appropriate Product Licences in place. | Choose an item |  |
|  | COMMERCIALISE OR USE DATA ONLY WITHIN AUSTRALIA | 3.2(b) | The Licensee may not Commercialise or otherwise use the Data except as permitted by clauses 3.1, 3.2(a) and 7.2(b), and then only within Australia. Note: Licensee may however, license *Derivative Products* to non-Australian domiciled customers (clause 7.2(b)). | Choose an item |  |
|  | DERIVATIVE PRODUCT – Government Statement | 3.3(b) | Every Derivative Product must enclose a notice (Copyright, accuracy, completeness, suitability) that complies with the Data Access Sub-Licence Agreement.  The Licensee confirms that appropriate Government Statements are included in each Derivative Product. | Choose an item |  |
|  | ACCESS TO DERIVATIVE PRODUCTS | 3.5(a) | The Licensee must provide to LSSA on an ongoing basis during the Term for contract management (e.g. licence checks) purposes, and at no charge to LSSA, a single copy of (or on-line access to) all Derivative Products that access the Data and any new products. | Choose an item |  |
|  | INFRINGMENT OF 3rd PARTY IP RIGHTS | 4.2(b) | The Licensee must notify LSSA as soon as practicable of any infringement, suspected infringement or alleged infringement by a Derivative Product of the Intellectual Property Rights of any person.  The Licensee has made all notifications required under this clause. | Choose an item |  |
|  | SECURITY AND INTEGRITY OF DATA | 7.1 | The Licensee must establish and maintain throughout the Term, privacy, security and other arrangements for ensuring compliance with its obligations under the Data Access Sub-Licence Agreement (which may include arrangements for auditing Customers' businesses in order to ensure compliance with the terms of Product Licences). | Choose an item |  |
|  | DATA STORAGE | 7.2(a) | The Licensee must ensure that the Data is stored and retained, electronically or otherwise, including storage on any server or other device, in Australia, and must not be stored, transported, distributed, maintained, accessed or supplied outside of Australia. | Choose an item |  |
|  | CHANGES TO DERIVATIVE PRODUCTS – major Changes | 10.4(a) | If the Licensee intends to implement a Change in the Derivative Products, it must promptly provide to LSSA, at no cost to LSSA a single copy of (or on-line access to) the Derivative Product the subject of the Change, full particulars in writing of the Change and without derogating from the Licensee's warranty in clause 10.2, LSSA must give the Licensee notification in writing that it is satisfied that the Change will not cause the Licensee to be in breach of that clause.  The Licensee has made all notifications required under this clause. | Choose an item |  |
|  | CHANGES TO DERIVATIVE PRODUCTS – Minor Changes | 10.4(b) | As soon as reasonably possible during the Term before it intends to or after a Minor Change is implemented, the Licensee must notify LSSA in writing of a Minor Change.  The Licensee has made all notifications required under this clause. | Choose an item |  |
|  | UNAUTHORISED USE | 11.2 | If the Licensee becomes aware that a Customer has used a Derivative Product, or any report or other thing generated by a Derivative Product, for a purpose not permitted by the Data Access Sub-Licence Agreement, or has done anything else not permitted by the Data Access Sub-Licence Agreement, the Licensee must immediately notify LSSA, in writing and in reasonable detail, of the unauthorised use or other act or omission.  The Licensee has made all notifications required under this clause. | Choose an item |  |
|  | NOTIFICATION REQUIREMENTS | 16 | The Licensee must notify LSSA in writing if any of the following events occur   1. if any director, secretary or officer of the Licensee is convicted of a criminal offence; 2. if the Licensee is or is likely to become insolvent or subject to insolvency proceedings; 3. if there is a change in control of the Licensee (whether by a change in majority shareholding or otherwise),   and such a notice must include such details of the event as LSSA may consider sufficient to enable LSSA to make an informed decision as to whether the Licensee will be able to continue to comply with the terms and conditions of the Data Access Sub-Licence Agreement.  The Licensee has made all notifications required under this clause. | Choose an item |  |
|  | SUPPLY OF DATA TO CONTRACTORS | 20.1 | The Licensee may, during the Term, disclose, distribute or supply the Data to a contractor (**Contractor**) engaged by the Licensee to carry out a task for or on behalf of the Licensee for the purposes set out in clauses 3.1(a) or 3.1(b), solely in relation to the Licensee's own Derivative Product, provided that the Licensee complies with the requirements in clause 20.1.  The Licensee has complied with this clause in all respects. | Choose an item |  |

1. **COMPLIANCE WITH DATA ACCESS SUB-LICENCE AGREEMENT (Security)**

Without limiting the above, the Licensee provides the following information on its compliance with the Data Access Sub-Licence Agreement in respect to security and integrity of the Data:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Item** | **Criteria** | **Clause No.** | **Summary of relevant Licence Condition** | **Licensee has fully complied with this requirement (Yes / No)** | **Details of any non-complying aspects and proposed remedies** |
|  | SECURITY AND INTEGRITY OF DATA – ISO Compliance | 7.1(e) | The Licensee must at all times comply with the AS/NZS ISO/IEC 27001 standard for Information Security Management Systems, as amended from time to time, in relation to the Data and Derivative Products.  The Licensee must annex a copy of its certification demonstrating that it has complied with the AS/NZS ISO/IEC 27001 (or similar security standard approved by LSSA) during the Compliance Period and respond to the questions in Items A.1 in Appendix C. | Choose an item |  |
|  | MINIMUM MANDATORY SPECIFICATIONS | 7.1 | If LSSA, and the Government, have approved that the Licensee is not required to be certified under AS/NZS ISO/IEC 27001 provided that, at all times, the Licensee has information security management systems, process and controls in place in relation to the Data and Derivative Products which comply with or exceed the Minimum Mandatory Specifications and are consistent with the Minimum Mandatory Specifications.  In confirming this requirement, regard must be given to the matters set out in Appendix C and supported by a 3rd party Technical Data Security Audit (undertaken by an independent 3rd party approved by LSSA and the Government). This report must provide an assessment of the implementation of the Licensee’s information security policies and procedures, including but not limited to:   * Risk Management: Confirmation that the Licensee’s Risk Management Framework has been implemented and relevant risks are being actively managed. * Information Security Management System: Confirmation that the Licensee’s Information Security policies, as outlined in their application, have been implemented. * Data Access and Protection Controls: Confirmation that the Data Access and Protection Controls defined in the Licensee’s application have been implemented and are actively managed. * Privacy: If any new or existing derivative products contain Personal Information not previously assessed, evidence that a new Privacy Impact Assessment (PIA) has been conducted.   A copy of the 3rd party Security Audit must be annexed to this Statement. | Choose an item |  |

**ANNEXURE A: DERIVATIVE PRODUCTS**

[**Insert current list of Derivative Products and call out any changes from any previously submitted list.**]

**ANNEXURE B: SECURITY AUDIT REPORT – PROGRESS OF RECOMMENDATIONS**

[**Insert progress of Security Audit Report Recommendations or insert “Not Applicable”.]**

**ANNEXURE C: MINIMUM MANDATORY SPECIFICATIONS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Number** | **Vendor Question** | **Notes for LSSA** | **Assurance Examples** |
| **A.1** | **ISO 27001 Certification** | | |
| A.1.1 | Does the Licensee have an ISMS certified to ISO 27001? |  | ISMS certification letter and audit report. |
| A.1.2 | Does the Licensee’s ISMS scope include derivative products that contain State Data? | The ISMS scope statement may not specify State Data or the Derivative Product as included. Further questioning and assurance should be sought to verify all State Data sits within the boundaries of the ISMS scope. | ISMS certification letter and audit report specifying scope of the ISMS. |
| A.1.3 | Does the Licensee’s ISMS meet the requirements outlined in the minimum mandatory specifications? |  | The Licensee’s Statement of Applicability is to demonstrate that the relevant ISO 27001 clauses that meet the Minimum Mandatory Specifications are specified as applicable and implemented. |
| **Provided that appropriate assurance has been provided for A.1.1, A.1.2 & A.1.3, a Licensee with an ISMS certified to ISO 27001 is not required to provide any further assurance of compliance such as that requested below.** | | | |
| **A.2** | **Information Asset Identification** | | |
| A.2.1 | Have all types of information within the Derivative Product been identified and documented? |  | - Evidence of an Information Asset Inventory/Register. - Asset identification report performed by Licensee or an independent third party. - Sanitised sample of information assets within the Derivative Product. |
| A.2.2 | Is there evidence that an assessment has been performed to identify whether the aggregation of State Data or any other Licensee data within the Derivative Product can result in the creation of personal information? | Refer to the OAIC for identifying personal information: https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information | - Assessment report performed by Licensee or an independent third party. - Attestation from Licensee confirming assessment has been performed and stating whether personal information exists within the Derivative Product. |
| A.2.3 | Is there any evidence that a competent and independent third party has verified and provided assurance that the findings of A.2.1 and A.2.2 meet the State’s Minimum Mandatory Specifications? | If independent assurance is not provided by a third party, LSSA is to either: 1) Ensure that the Licensee/applicant gets an independent assessment/verification performed; or 2) Internally determine whether the findings provided by the Licensee/applicant provide sufficient assurance of meeting the Minimum Mandatory Specifications. | - Asset identification and assessment report performed by an independent third party. - Evidence collection and assessment performed by LSSA (if required). |
| **A.3** | **Risk Management** | | |
| A.3.1 | Does the Licensee have a formalised Risk Management Framework that is aligned with international standards? |  | Licensee’s should have a documented Risk Management Framework, Policy or Procedure that: - is aligned to ISO 31000;  - specifies how the VAR manages information security risks within the organisation; and - has documented its risk acceptance criteria. |
| A.3.2 | Has the Licensee performed an information security risk assessment of the Derivative Product? | At a minimum, the risk assessment should identify a number of risks to State Data that the Minimum Mandatory Specification controls address. | Licensee’s should have a risk assessment report of the derivative product, performed by the Licensee or an independent third party, that specifies controls to be applied to mitigate risks identified. |
| A.3.3 | Is there a Corrective Action plan?  Does this plan specify how and when controls identified within the Information Security Risk Assessment will be implemented? |  | Corrective Action plan to remediate issues where a Licensee is not meeting the expected obligations of LSSA and the State under the Data Access Sub-Licence Agreement. |
| A.3.4 | Is there any evidence that a competent and independent third party has verified and provided assurance that the findings of A.3.1, A.3.2 and A.3.3 meet the State’s Minimum Mandatory Specifications? | If independent assurance is not provided by a third party, the State is to either: 1) Ensure that the Licensee/applicant gets an independent assessment/verification performed; or 2) Internally determine whether the findings provided by the Licensee/applicant provide sufficient assurance of meeting the Minimum Mandatory Specifications. | - Risk assessment report performed by an independent third party. - Evidence collection and assessment performed by LSSA (if required). |
| **A.4** | **Leadership Support** | | |
| A.4.1 | Does the Licensee have an approved Information Security Policy that has been published and communicated to all employees? | Information Security Policy should: 1) Indicate the organisation’s commitment to protecting its information assets; 2) Provide high-level information security objectives of the organisation; 3) Provide a commitment to meeting these information security objectives;  4) Provide a commitment to the continuous improvement of information security within the organisation. | - Published Information Security Policy. - Evidence of approval by Management. |
| **A.5** | **Workforce Management** | | |
| A.5.1 | Does the Licensee perform adequate background checks of new employees and contractors who have access to State Data? | Ensure background checks are performed to verify the character and bona fides of Licensee employees or third parties who have access to State Data.  If the Derivative Product contains personal information, police checks must be performed. | - Employee reference check of a recent hire - Right to work in Australia confirmed for a recent hire - Police background check of a recent hire |
| A.5.2 | Are Licensee employees, third parties and contractors aware of the acceptable use of State Data within the Derivative Product. |  | - Acceptable Use Policy. - Evidence that employees, third parties and contractors have read and acknowledged the acceptable use of State Data. |
| A.5.3 | Is there a formalised disciplinary process for managing employees that have committed an information security breach or breach of the Licensee’s Acceptable Use Policy? |  | - Disciplinary procedure or evidence in employee contracts. |
| **A.6** | **Requirements of Access Control and Protection of Data** | | |
| A.6.1 | Is there a formalised access control policy? Does it meet the requirements specified within the Mandatory Minimum Specifications? | Required in order to enforce a minimum set of access control requirements that take into consideration the State’s low appetite for unauthorised access, disclosure or modification of State Data.  To avoid confusion and duplication of access control requirements, integrate access control requirements within protection of State Data. | - Access Management Policy is in place. |
| A.6.2 | Is there a formal process covering the registration and de-registration of employees for access rights and network access? | Required in order to enforce a minimum set of access control requirements that take into consideration the State’s low appetite for unauthorised access, disclosure or modification of State Data.  To avoid confusion and duplication of access control requirements, integrate access control requirements within protection of State Data. | - Procedure on onboarding and offboarding of staff. - Procedure for assigning and revoking user access rights. - User access request ticket number from a service management system with approval from manager to provide access. |
| A.6.3 | Is access to State Data limited to individuals within Australia? | Access shall be limited to individuals within Australia as specified within 7.2(a) of the Data Access Sub-Licence Agreement | - Validation or evidence of Licensee employee/individuals who access State Data reside within Australia.  - Evidence of third party agreements restricting third party access to State Data to within Australia. |
| A.6.4 | Is allocation and use of access rights with high level privileges restricted and controlled? | To ensure that high level privileges are only provided to a limited number of personnel who have a genuine business for elevated privileges. | - Access Management Policy that includes management of privileged access rights. - Evidence of penetration test of authorised/unauthorised users attempting privilege escalation of Derivative Product. |
| A.6.5 | Are user access rights regularly reviewed? | Required in order to enforce a minimum set of access control requirements that take into consideration the State’s low appetite for unauthorised access, disclosure or modification of State Data.  To avoid confusion and duplication of access control requirements, integrate access control requirements within protection of State Data. | - Calendar item for a review of user rights on a regular basis. - Evidence of a recent user access review including user and administrator accounts. |
| A.6.6 | Is there a formalised password policy which requires users to follow the Licensee’s practices when it comes to the use and management of passwords? | Required in order to enforce a minimum set of access control requirements that take into consideration the State’s low appetite for unauthorised access, disclosure or modification of State Data.  To avoid confusion and duplication of access control requirements, integrate access control requirements within protection of State Data. | - Password Policy with defined password standards. |
| A.6.7 | Are physical security perimeters defined and used to limit unauthorised access and protect areas that contain:  - Network equipment that transit State Data; - Systems that hold State Data; or - Hard copies of State Data? | To enforce a minimum set of access control requirements that take into consideration the State’s low appetite for unauthorised access, disclosure or modification of State Data.  To avoid confusion and duplication of access control requirements, integrate access control requirements within protection of State Data. | - Physical Security Policy. - Clear desk and clear screen policy. - Register of building access cards. - Evidence of physical controls implemented. |
| A.6.8 | Is only sanitised data used in the environment where testing of Derivative Products is performed? | Ensure live data is not used in a testing environment where controls may not meet security requirements. | - Evidence that only sanitised test data provided by the State is used for testing Derivative Products. |
| A.6.9 | Does the Licensee conform to the copyright and data integrity requirements set out by the State? |  | - Evidence of use of warning and copyright statements specified within the Data Access Sub-License Agreement. |
| A.6.10 | Are there appropriate controls to protect the confidentiality of personal information at rest or in transit? | It is expected that the Licensee will implement appropriate protection of data based on risks identified within the information security risk assessment. | - Proof of appropriate encryption used. - Access control mechanisms for Personal Information in place.  - Penetration test of Derivative Product. |
| **A.7** | **Privacy** | | |
| A.7.1 | If Personal Information has been identified within the derivative product, has the VAR performed a Privacy Impact Assessment (PIA) aligned with the *Privacy Act 1988* (Cth) and the underlying Australian Privacy Principles (**Privacy Laws**)? Are all information security control identified within the PIA included, where applicable, within the information security risk assessment (Assessment Number A.3.2)? | Provide assurance that appropriate controls are in place on the requirements for privacy. | - Evidence a Privacy Impact Assessment has been conducted and assessed against the Privacy Laws. - Resultant information security controls derived from assessment are considered in the Risk Assessment of the Derivative Product. |
| A.7.2 | Has the Licensee performed a Privacy Impact Assessment (**PIA**) conducted for a Derivative Product that contains personal information? | Provide assurance that appropriate controls are in place on the requirements for privacy. | - Evidence a Privacy Impact Assessment has been conducted and assessed against the Privacy Laws. - Resultant information security controls derived from Privacy Impact Assessment are considered in the Risk Assessment of the Derivative Product. |
| A.7.3 | Is there an implemented incident response plan that will inform LSSA of any breach of State Data within 24 hours? | To ensure LSSA is advised within 24 hours should a data breach occur that involves State Data. | Incident Response Plan that includes direct references to data breaches and is aligned with the Notifiable Data Breaches component of the Privacy Act. |

1. Insert date of most recent Security Audit Report (if applicable). [↑](#footnote-ref-2)