Australian Government
Department of Education

PRISMS API Services Terms of Use for Software Vendors

Provider Registration and International Student Management System (PRISMS)

Contents

PRISMS API Services Terms of Use – Software Vendors

1. About these Terms

1.1 In these Terms, a reference to:

(a) **Change in Control** means:

(i) a body corporate or entity that Controls the Provider ceases to Control the Provider; or

(ii) a body corporate or entity that does not Control the Provider comes to Control the Provider.

(b) **Client ID(s)** means the unique identifier created by the Department which allows a Provider to use the PRISMS API with a specific Recognised PRISMS Integrated Software. Each Recognised PRISMS Integrated Software used by a Provider requires its own Client ID.

(c) **Control** means, in relation to the Vendor in the context of a Change in Control, any of the following:

(i) the ability to exercise or control the exercise of the right to vote in respect of more than 50% of the voting shares or other form of voting equity in the Vendor;

(ii) the ability to dispose or exercise control over the disposal of more than 50% of the shares or other form of equity in the Vendor;

(iii) the ability to appoint or remove a majority of the directors of the Vendor;

(iv) the ability to exercise or control the exercise of the casting of a majority of votes at the meeting of the board of directors of the Vendor; and

(v) any other means, direct or indirect, of dominating the decision making and financial and operating policies of the Vendor.

(d) **Cyber Security Assessment** is a reference to the evaluation used by the Department to ensure a Vendor Software Application meets the security standards set out in the Right Fit for Risk Cyber Security Accreditation Framework.

(e) **Cyber Security Assessment Outcome** means the rating given to a Vendor Software Application as a result of a Cyber Security Assessment, reflecting the level of cyber security risk associated with the Vendor Software Application.

(f) **CRICOS** means Commonwealth Register of Institutions and Courses for Overseas Students.

(g) **Department** is a reference to the Commonwealth of Australia as represented by the Department of Education.

(h) **Eligible Data Breach** has the same meaning as in the Privacy Act.

(i) **ESOS Act** is a reference to the *Education Services for Overseas Students Act 2000* (Cth).

(j) **Personal Information** has the same meaning as in the Privacy Act.

(k) **PRISMS** means the Department's Provider Registration and International Student Management System.

(l) **PRISMS API** is a reference to the Department's application programming interface for PRISMS that allows Providers to access and enter information into PRISMS for the purposes of section 109 of the ESOS Act.

(m) **PRISMS API Portal** is a reference to the online platform provided by the Department and accessible at https://portal.api.prisms.education.gov.au/ (or such other website as notified by the Department from time to time) to enable software vendors to access, discover, and learn about the PRISMS API Services.

(n) **PRISMS API Services** is a reference to:

  (i) the PRISMS API Portal;

  (ii) the PRISMS API;

  (iii) the PRISMS Staging Environment;

  (iv) the PRISMS Staging Environment Website; and

  (v) if the Department has granted a Vendor Software Application access to the PRISMS API in the PRISMS Production Environment, access to the PRISMS API in the PRISMS Production Environment.

(o) **PRISMS API Services Hub** is a reference to the Department's website accessible at https://www.education.gov.au/prisms-api-services-hub (or such other website as notified by the Department from time to time) which provides general information about the PRISMS API Services, including:

  (i) updates, news and communications;

  (ii) the process for software vendors and education providers to gain access to the PRISMS API Services; and

  (iii) the requirements that must be met for a vendor's software application to be recognised as PRISMS-integrated software by the Department.

(p) **PRISMS Production Environment** is a reference to the live environment in which education providers access and enter information for the purposes of section 109 of the ESOS Act. The Vendor's Providers will use the Vendor's Recognised PRISMS-Integrated Software to perform transactions in the PRISMS Production Environment.

(q) **PRISMS Staging Environment** is a reference to the test environment provided to software vendors by the Department to test the integration of their software to the PRISMS API in a production-like- setting.

(r) **PRISMS Staging Environment Website** means the instance of the PRISMS web application available in the PRISMS Staging Environment.

(s) **Privacy Act** means the *Privacy Act 1988* (Cth).

(t) **Provider** means an education provider registered with the CRICOS under the ESOS Act who uses any product developed, marketed or promoted by the Vendor which uses the PRISMS API.

(u) **Recognised PRISMS-Integrated Software** means a Vendor Software Application that has been recognised by the Department as having successfully completed integration with PRISMS in the PRISMS Staging Environment and which meets the required standards to connect to the PRISMS Production Environment.

(v) **Right Fit for Risk Cyber Security Accreditation Framework** means the framework developed by the Commonwealth Department of Employment and Workplace Relations (DEWR) as amended from time to time which the Department uses for the Cyber Security Assessment.

(w) **Terms** means these PRISMS API Terms of Use as amended from time to time in accordance with clause 1.3.

(x) **Vendor** is a reference to the entity agreeing to these Terms whose details are set out in the Vendor Details section of these Terms.

(y) **Vendor Personnel** is a reference to Vendor officers, employees, contractors, agents and any other person over whom the Vendor exercise control or direction.

(z) **Vendor Software Application** is a reference to the software application(s) developed or used by the Vendor to integrate with or use the PRISMS API, as identified in the Vendor Details section of these Terms or approved by the Department under clause 2.5.

1.2 These Terms set out the basis on which the Vendor undertakes to access the PRISMS API Services. The Vendor acknowledges and agrees that if the Department provides it with access to the PRISMS API Services in accordance with these Terms, that access is given to the Vendor in consideration of its agreement to these Terms.

1.3 The Department may amend these Terms with at least 2 weeks notice to the Vendor which:

(a) sets out the updated Terms; and

(b) the date that updated Terms will take effect.

1.4 The parties acknowledge and agree that the Department may provide a notice under clause 1.3 by:

(a) publishing updated Terms on the PRISMS API Services Hub or the PRISMS API Portal; or

(b) sending the updated Terms to the Vendor's e-mail address (as set out in the Vendor Details section of these Terms or as otherwise updated by the Vendor).

1.5 If the Vendor accesses or uses the PRISMS API Services after the notice period, it will be taken to agree to the amended Terms.

---

2. Vendor Access to the PRISMS API Portal, the PRISMS Staging Environment Website and the PRISMS API in the PRISMS Staging Environment

2.1 As at the commencement of these Terms, the Vendor has submitted to the Department a request to access:

(a) the PRISMS API Portal;

(b) the PRISMS Staging Environment Website; and

(c) the PRISMS API in the PRISMS Staging Environment,

in connection with one or more Vendor Software Application(s) and the Vendor represents and warrants to the Department that any information the Vendor has provided, or will provide, to the Department in connection with that request is true, complete and accurate.

2.2 The Department will determine (at its sole discretion) whether to grant or refuse the Vendor or Vendor Personnel access to the PRISMS API Portal, the PRISMS Staging Environment Website and the PRISMS API in the PRISMS Staging Environment in connection with the Vendor Software Application(s).

2.3 The Department may grant the Vendor (and Vendor Personnel) access to the PRISMS Staging Environment Website and the PRISMS API in the PRISMS Staging Environment subject to conditions that are in addition to the conditions set out in these Terms, and the Vendor must comply with those conditions. The Department will notify the Vendor of the outcome of its application but is not required to provide reasons for its decision.

2.4 If the Vendor is granted access to the PRISMS Staging Environment Website and the PRISMS API in the PRISMS Staging Environment, that access is strictly limited to the specific Vendor Software Application the subject of the Department's grant of access.

2.5 If the Vendor seeks to access the PRISMS Staging Environment Website and the PRISMS API in the PRISMS Staging Environment in connection with a different Vendor Software Application (**New Vendor Software Application**), the Vendor must obtain the Department's prior written approval to do so. The Department will notify the Vendor of the Department's decision but is not required to provide reasons for its decision. The Department may approve the grant of access in connection with a New Vendor Software Application subject to conditions that are in addition to the conditions set out in these Terms, and the Vendor must comply with those conditions.

2.6 The Vendor acknowledges that:

(a) granting access to the PRISMS API Portal, the PRISMS Staging Environment Website and/or the PRISMS API in the PRISMS Staging Environment; or

(b) approving the grant of access in connection with a New Vendor Software Application,

does not indicate or imply that the Vendor Software Application will be Recognised PRISMS-Integrated Software.

2.7 Where requested by the Department, the Vendor must provide the Department with a copy of the Vendor Software Application(s) the subject of a request referred to in clause 2.1 or 2.5.

---

3. Vendor Software Application access to the PRISMS API in the PRISMS Production Environment

3.1 To access and connect with the PRISMS API in the PRISMS Production Environment, a Vendor Software Application must be Recognised PRISMS-Integrated Software, which involves:

(a) the Vendor:

(i) having an approach for managing X.509 security certificates generated through the Australian Government's Relationship Authorisation Manager (available at: https://authorisationmanager.gov.au/#/login);

(ii) completing integration with PRISMS in the PRISMS Staging Environment specific to that application;

(iii) successfully testing the integration of the Vendor Software Application with the PRISMS API in the PRISMS Staging Environment;

(iv) submitting to the Department an application for the Vendor Software Application to be Recognised PRISMS-Integrated Software; and

(v) providing any additional information requested by the Department to enable the Department to assess the Vendor's suitability to be granted access to the PRISMS API in the PRISMS Production Environment; and

(b) the Department:

(i) reviewing the Vendor's request and any other relevant information to determine whether the Vendor satisfies the eligibility criteria (available on the PRISMS API Services Hub or as otherwise notified by the Department and as amended from time to time) for the Vendor Software Application to operate in the PRISMS Production Environment; and

(ii) undertaking a recognition process, which includes an assessment to ensure that the Vendor Software Application is ready to connect to the PRISMS Production Environment.

3.2 The Department will notify the Vendor of the outcome of its application for a Vendor Software Application to be Recognised PRISMS-Integrated Software but is not required to provide reasons for its decision.

3.3 The Department will determine (at its sole discretion) whether to grant or refuse a Vendor Software Application access to the PRISMS API in the PRISMS Production Environment.

3.4 The Department may grant a Vendor Software Application access to the PRISMS API in the PRISMS Production Environment subject to conditions that are in addition to the conditions set out in these Terms, and the Vendor must comply with those conditions.

3.5 The Department may advise the Vendor at any time and at its sole discretion, that the Vendor must:

(a) have their Recognised PRISMS-Integrated Software reassessed by the Department in order for it to continue accessing the PRISMS API, including (but not limited to) when the PRISMS API undergoes a major version change; or

(b) make changes to their Recognised PRISMS-Integrated Software in order to continue accessing the PRISMS API, including when the Department believes that the Recognised PRISMS-Integrated Software is resulting in unintended behaviour in the PRISMS API (e.g., it does not institute a student search correctly).

3.6 If a Vendor Software Application is granted access to the PRISMS API in the PRISMS Production Environment, the Vendor:

(a) must promptly advise the Department of any changes to the Vendor Software Application, or the services the Vendor provides to Providers, that might change the information provided by the Vendor to the Department in connection with the Vendor's application for the Vendor Software Application to be Recognised PRISMS-Integrated Software (including any information in the Vendor's production vendor software access request form); and

(b) agrees that the Department may disclose publicly the name of the Vendor and details of its Recognised PRISMS-Integrated Software.

---

4. Use of the PRISMS API Services

4.1 The Vendor must not, and the Vendor must ensure that Vendor Personnel and any Providers do not, use the PRISMS API Services (including the PRISMS API) for any activity which:

(a) constitutes a breach of any law;

(b) is prohibited by these Terms;

(c) is likely to cause loss or damage to any person, the PRISMS API Services or the Department's systems or data;

(d) transmits any viruses, worms, defects, Trojan horses, malware or any code of a destructive manner; or

(e) reverse engineers or attempts to extract source code from the PRISMS API.

4.2 The Vendor must ensure that it complies, and that Vendor Personnel comply, with the data security, privacy, system integrity and other requirements specified in the Vendor Use Policy (as published on the PRISMS API Portal and as amended from time to time).

4.3 The Department may provide resources to the Vendor in relation to the PRISMS API Services. The Vendor acknowledges and agrees that the Department is not responsible for any loss or damage caused by any reliance on, or use made of, those resources by the Vendor or a Provider.

4.4 The Vendor must diligently and promptly correct any bugs or faults in Recognised PRISMS-Integrated Software that cause it to incorrectly access the PRISMS API or display PRISMS API content incorrectly.

4.5 The Vendor acknowledges that the Department monitors and collects information about all actual or attempted access to, and activity within, the PRISMS API in the PRISMS Production Environment and the PRISMS Staging Environment. The Vendor must provide any information requested by the Department in relation to its access to and use of the PRISMS API Services, including, but not limited to, API access logs.

4.6 The Vendor is responsible for maintaining up-to-date and accurate information with the Department (including a current e-mail address and other contact information required by the Department).

4.7 The Department will not charge a fee for:

(a) the Vendor or Vendor Personnel accessing the PRISMS API Portal, the PRISMS Staging Environment Website or the PRISMS API in the PRISMS Staging Environment; or

(b) Recognised PRISMS-Integrated Software accessing the PRISMS API in the PRISMS Production Environment.

4.8 The development and use of the Vendor Software Application and the performance of the Vendor's obligations under these Terms are at the Vendor's sole cost and expense.

---

5. Privacy

5.1 The Vendor must comply with all applicable privacy laws, including the Privacy Act.

5.2 The Vendor must comply with, and ensure that Vendor Personnel comply with, any privacy policy or guidelines notified to the Vendor by the Department from time to time.

5.3 The Vendor must immediately notify the Department if any of the following occur:

(a) the Vendor receives a complaint from a third party (including a Provider) about the handling of any Personal Information in connection with PRISMS or the PRISMS API Services;

(b) the Vendor breaches its obligations under this clause 5 or becomes aware of circumstances that may reasonably suggest that it could have breached its obligations under this clause; or

(c) the Privacy Commissioner in any Australian jurisdiction requests information about or commences an investigation in relation to the PRISMS API Services.

5.4 The Vendor must comply with any reasonable direction from, the Department, in connection with any potential or actual breach of privacy, including without limitation, unauthorised access to Personal Information in connection with the Vendor's use of the PRISMS API Services.

5.5 If the Vendor suspects that there may have been an Eligible Data Breach in relation to any Personal Information held by the Vendor as a result of the Vendor Software Application's access to the PRISMS API (including data retrieved via the PRISMS API), the Vendor must:

(a) immediately report it to the Department and provide a written report within 3 days; and

(b) where requested by the Department, carry out an assessment in accordance with the requirements of the Privacy Act.

5.6 If the Vendor is aware that there has been an Eligible Data Breach in relation to any Personal Information held by the Vendor as a result of the Vendor Software Application's access to the PRISMS API (including data retrieved via the PRISMS API), the Vendor must:

(a) take all reasonable action to mitigate the risk of the Eligible Data Breach causing serious harm to any individual to whom the Personal Information relates;

(b) take all other action necessary to comply with the requirements of the Privacy Act; and

(c) take any other action as reasonably directed by the Department.

5.7 The Vendor must ensure that all Vendor Personnel who access or use Personal Information in connection with the API Services are informed about the Vendor's obligations under this clause 5.

---

6. Security and data protection

6.1 The Vendor must:

(a) implement safeguards to prevent unauthorised access, misuse, or corruption of data exchanged through the PRISMS API in the PRISMS Production Environment;

(b) take all reasonable steps to manage the risk that the Vendor's use of the PRISMS API, or a Vendor Software Application's interaction with the PRISMS API, introduces viruses, malicious computer code or other interference which may damage the Vendor Software Application or the Vendor's systems;

(c) comply, and ensure Vendor Personnel comply with the Vendor Use Policy (as published on the PRISMS API Portal and as amended from time to time) and any other directions or Department or Commonwealth policies as notified to the Vendor from time to time;

(d) ensure that no Provider Username and Password are stored in any Vendor Software Application;

(e) ensure that any Provider data stored in or in connection with Recognised PRISMS-Integrated Software is securely stored and strictly segregated to ensure that each Provider can only access its own data;

(f) maintain a Cyber Security Assessment Outcome of a suitable standard as determined by the Department to maintain access to the PRISMS API;

(g) once a Vendor Software Application is Recognised PRISMS Integration-Software, undertake a Cyber Security Assessment of the Vendor Software Application every 3 years;

(h) on request of the Department, complete a new cyber security assessment questionnaire; and

(i) subject to clause 6.2, delete and destroy all data retrieved via the PRISMS API (including Provider credentials (such as Client ID(s)) that the Vendor holds for a Provider within 30 days of:

(i) the Provider notifying the Vendor that it wants to cease using the Vendor Software Application in connection with PRISMS; or

(ii) on the Provider's request,

and the Vendor must promptly notify the Department and the Provider when the data has been deleted and destroyed.

6.2 Nothing in clause 6.1(i) requires the Vendor to delete or destroy data relating to a Provider if doing so would cause the Vendor to breach an obligation to retain data in an agreement between the Vendor and that Provider. Where such an agreement exists, the Vendor must notify the Department of the relevant agreement and confirm that all other data which the Vendor is not expressly required to retain under the agreement has been deleted and destroyed in accordance with clause 6.1(i).

---

7. Technical Support

7.1 The PRISMS API Services and the PRISMS API Services Hub are provided 'as is', with limited technical support available by the Department. Vendors are required to undertake development and maintenance of PRISMS API connectivity utilising their own resources.

7.2 To support development, the Department will provide:

(a) access to the PRISMS API Portal to provide secure access to information required to develop and maintain access to the PRISMS API Services;

(b) up to date technical documentation through the PRISMS API Portal;

(c) access to limited technical support (as described on the PRISMS API Portal) via the PRISMS API helpdesk available at PRISMSAPI@education.gov.au.

---

8. Continuity of access

8.1 The Department provides the Vendor and any Provider with access to the PRISMS API Services on an "as is" and "as available" basis. The Department does not warrant that access to the PRISMS API Services by the Vendor or any Provider will be continuous or fault free. However, the Department will use reasonable endeavours to provide a consistent level of service.

8.2 The Vendor must promptly report to the Department:

(a) any loss of, or fault in, the Vendor's access to the PRISMS API (unless the Department has issued a notification of a current PRISMS API outage); and

(b) any event which compromises, may compromise, or may have compromised the security or integrity of the PRISMS API or the Department's servers, systems or networks providing the PRISMS API, or any of the Department's or a Provider's data.

8.3 The Vendor must provide all assistance reasonably requested by the Department to respond to and protect against a risk to the security or integrity of the PRISMS API Services and any of the Department's servers, systems, networks or data.

8.4 The Department may modify or alter the PRISMS API at any time without notice. However, the Department will endeavour to publish planned updates to the PRISMS API on the PRISMS API Portal. The Department does not guarantee that new versions of the PRISMS API will be backwards compatible.

---

9. Circumstances to be notified to the Department

9.1 Without limiting the Vendor's other obligations under these Terms, the Vendor must promptly notify the Department if:

(a) material changes are made to any Recognised PRISMS-Integrated Software, including significant changes to the underlying code base;

(b) the Vendor changes, or intends to changes, the hosting solution for any of its Recognised PRISMS-Integrated Software, including movement from on premises to cloud, or between cloud providers;

(c) the Vendor becomes aware of a defect or fault in any of its Recognised PRISMS-Integrated Software or the PRISMS API which is resulting in unintended behaviour in the PRISMS API;

(d) the Vendor becomes aware that a Provider no longer wishes to use the PRISMS API through any of its Recognised PRISMS-Integrated Software;

(e) the Vendor experiences a Change in Control;

(f) the Vendor becomes insolvent or comes under one of the forms of external administration referred to in chapter 5 of the *Corporations Act 2001* (Cth), or has an order made against it for the purpose of placing it under external administration;

(g) the Vendor has been subject to a cybersecurity or data breach incident requiring reporting to the Australian Signals Directorate Australian Cybersecurity Incident Centre or the Office of the Australian Information Commissioner;

(h) the Vendor becomes aware that a Provider has been subject to a cybersecurity or data breach incident requiring reporting to the Australian Signals Directorate Australian Cybersecurity Incident Centre or the Office of the Australian Information Commissioner; and

(i) the Vendor is subject of investigation by a law enforcement or regulatory agency.

10. Intellectual property

10.1 The Department grants the Vendor a revocable, non-transferable, non-exclusive licence to use the PRISMS API:

(a) for so long as these Terms remain on foot and the Vendor's access to the PRISMS API Services have not been suspended; and

(b) solely for the purpose of the Vendor integrating the Vendor Software Application with PRISMS and providing the Vendor Software Application and associated services to Providers.

10.2 The Vendor does not acquire ownership of any rights in the PRISMS API Services, in any of the logos, designs or marketing material referred to in clause 10.4, or any of the data accessed by using the PRISMS API Services.

10.3 The Vendor:

(a) acknowledges and agrees that all data retrieved via the PRISMS API remains the property of the Department; and

(b) warrants that it has received a sublicence from each Provider to the extent necessary to use the data retrieved via the PRISMS API for the purposes of providing the Vendor Software Application and associated services to Providers.

10.4 The Department grants the Vendor, subject to any direction by the Department, a revocable, non-transferable, non-exclusive licence to use any logos, designs and marketing materials made available by the Department via the PRISMS API Portal or the PRISMS API Services Hub:

(a) for so long as these Terms remain on foot and the Vendor's access to the PRISMS API Services has not been suspended; and

(b) solely for the purpose of the Vendor performing marketing and communications activities in connection with the Vendor's Recognised PRISMS Integrated Software.

10.5 The Vendor acknowledges and agrees that:

(a) its use of the term ‘Recognised PRISMS Integrated Software’ in any marketing and communications activities in connection with the Vendor's Recognised PRISMS Integrated Software is conditional upon the Vendor's access to the PRISMS API having not been suspended or terminated; and

(b) it will cease using the term ‘Recognised PRISMS Integrated Software’ in any marketing and communications activities in connection with the Vendor's Recognised PRISMS Integrated Software if the Vendor's access to the PRISMS API is suspended or terminated.

10.6 By accessing the PRISMS Staging Environment, the Vendor grants to the Department a revocable, non-exclusive licence (including the right to sublicence) to use the Vendor Software Application for the purpose of the Department conducting validation and integration testing within the PRISMS Staging Environment.

10.7 By accessing the PRISMS API, the Vendor grants to the Department a revocable, non-exclusive licence (including the right to sublicence) to collect, use and disclose the information the Vendor provides through the PRISMS API for:

(a) the purposes of facilitating access to the PRISMS API; and

(b) any other use which is permitted by law.

10.8 If the Vendor revokes the licence referred to in clause 10.7, the parties acknowledge and agree that the Terms will, by mutual agreement, be immediately terminated.

---

11. Liability and indemnity

11.1 The Vendor acknowledges and agrees that:

(a) it uses the PRISMS API Services at its own risk;

(b) the Department may change and evolve PRISMS and the PRISMS API Services over time which may require the Vendor to make changes to the Vendor Software Application(s) to continue using the PRISMS API Services, and the Department will have no liability whatsoever for any costs incurred by the Vendor in making changes to the Vendor Software Application(s);

(c) the development and use of the Vendor Software Application(s), including any changes required to Recognised PRISMS-integrated Software, are at the Vendor's sole cost and expense; and

(d) to the extent permitted by law, the Department is not liable to the Vendor, Vendor Personnel or Providers for any loss or damage (however described) that is directly or indirectly related to:

(i) accessing or using the PRISMS API Services or the PRISMS API Services Hub; or

(ii) the unavailability or performance of any of the PRISMS API Services or the PRISMS API Services Hub.

11.2 The Vendor agrees to indemnify the Department for any loss or damage (however described) suffered by the Department or a third party arising from or related to:

(a) any flaw or defect (whether caused by negligence or not) in a Vendor Software Application;

(b) any breach of intellectual property rights by the Vendor or Vendor Personnel; or

(c) any breach by the Vendor or Vendor Personnel of these Terms.

11.3 The Vendor's liability to indemnify the Department will be proportionately reduced to the extent that the Department contributed to the relevant loss or damage.

---

12. Suspension and termination of access

12.1 These Terms will terminate immediately if the Department rejects the Vendor's application referred to in clause 2.1.

12.2 The Department may by notice immediately suspend or terminate the Vendor's access to some, or all, parts of the PRISMS API Services and in relation to some or all of the Vendor Software Applications:

(a) if the Department believes or suspects that the Vendor has breached these Terms;

(b) if the Department believes or suspects that the Vendor's access to the PRISMS API Services, including via any Vendor Software Application, compromises, may compromise, or may have compromised the security or integrity of the PRISMS API Services or any of the Department's servers, systems, networks or data;

(c) if the Vendor fails to:

(i) have relevant parts of any Recognised PRISMS-Integrated Software re-assessed as requested by the Department; or

(ii) make required updates to any Recognised PRISMS-Integrated Software,

in response to a major software change to the PRISMS API; or

(d) for any other reason, including without limitation, where the Department believes there is a flaw or defect in a Vendor Software Application.

12.3 The Department is not responsible for any loss caused by the suspension or termination of the Vendor's access to the PRISMS API Services in accordance with these Terms, including any liability that the Vendor has to a Provider.

12.4 If the Department suspends the Vendor's access to the PRISMS API Services under clause 12.2 the Vendor must, unless otherwise specified in the suspension notice:

(a) immediately stop using the PRISMS API Services (or that part of the PRISMS API Services for which access is suspended);

(b) immediately stop any Provider from using the PRISMS API via a Vendor Software Application; and

(c) not onboard any new Providers into the PRISMS API.

12.5 If the Department terminates the Vendor's access to the PRISMS API Services:

(a) the Vendor must immediately stop using the PRISMS API Services (or that part of the PRISMS API Services or in connection with those Vendor Software Applications for which access is terminated);

(b) unless otherwise specified in the termination notice, the Vendor must:

(i) immediately delete all temporarily cached information related to the PRISMS API Services;

(ii) immediately destroy all confidential information specified by the Department in the termination notice; and

(iii) subject to clause 12.6, delete and destroy all data retrieved through the PRISMS API Services, including any CRICOS registration data, student data, enrolment data, Provider credentials (such as Client ID(s)) and agent data;

(c) the Department may audit the Vendor to ensure it has undertaken all required actions set out in this clause 12.5; and

(d) unless otherwise specified in the termination notice, the Department will withdraw access to the PRISMS API for all Providers that were accessing the PRISMS API through the Vendor Software Application.

12.6 For avoidance of doubt, Vendor is not required to delete or destroy data relating to a Provider if doing so would cause the Vendor to breach an obligation to retain data in an agreement between the Vendor and that Provider. Where such an agreement exists, the Vendor must notify the Department of the relevant agreement and confirm that all other data which the Vendor is not expressly required to retain under the agreement has been deleted and destroyed in accordance with the termination notice.

12.7 The Vendor may stop using the PRISMS API Services at any time by providing 14 days' notice to the Department.

12.8 If the Vendor wants to terminate these Terms, the Vendor must provide the Department with prior written notice and upon termination, cease accessing or using the PRISMS API Services, and ensure that Vendor Personnel and any Providers cease accessing or using the PRISMS API via any Vendor Software Application.

---

13. Auditing

13.1 The Department may at any time without notice undertake an audit of the Vendor's compliance with these Terms.

13.2 As part of any audit conducted under clause 13.1, where requested, the Vendor must promptly (and within the timeframe requested by the Department):

(a) provide the Department with documentation regarding the Vendor's organisation and any Vendor Software Application;

(b) demonstrate to the Department the functionality of a Vendor Software Application; and

(c) provide the Department with user access to any Vendor Software Application in a demo or test account.

13.3 Failure by the Vendor to comply with a request under clause 13.2 may result in the suspension or termination of the Vendor's access to PRISMS API Services.

---

14. Governing law

14.1 These Terms are governed by the law in force in the Australian Capital Territory, Australia.

14.2 The Vendor agrees to submit to the non-exclusive jurisdiction of the courts of the Australian Capital Territory, Australia in respect of any dispute under these Terms.

---

15. Execution

15.1 By signing the Vendor agrees to be bound by these Terms.

Vendor Details

Vendor Info	Details
Vendor’s legal name:	
Vendor’s ACN:	
Vendor’s ABN:	
Vendor’s email:	
Vendor’s postal address:	
Vendor’s representative:	
Vendor Software Application(s):	

EXECUTED as a DEED POLL

Option 1: Use this execution block if the Vendor is a company incorporated under the Corporations Act.

Executed by **[*insert full name and ABN of Vendor*]** in accordance with section 127 of the Corporations Act 2001 (Cth):

Signature of director	Signature of company secretary/director (print)
Full name of director	Full name of company secretary/director (print)
Full name of director	Full name of company secretary/director (print)
Date	Date

Option 2: Use this execution block if the Vendor is not a company incorporated under the Corporations Act.

Signed, sealed and delivered by **[*insert full name and ABN (if applicable) of Vendor*]** in the presence of:

Signature of witness	Signature of individual / authorised representative
Full name of witness (print)	Full name of individual / authorised representative (print)
	Position of authorised representative (print)
Date	