

API Centre Terms and Conditions

25 May 2026

Version 15.0

Contents

API Centre Terms and Conditions Introduction	4
1. Defined terms and interpretation	4
1.1 Defined terms	4
1.2 Legal Parties	11
1.3 Interpretation	11
2. Application of Terms	12
3. Registration of API Standards Users	12
4. API Centre role	12
4.1 The API Centre will, in accordance with these Terms:	12
4.2 The API Centre may, in accordance with these Terms:	13
5. Setting the Annual API Standards User Fee	14
5.1 Board will set Annual API Standards User Fee	14
6. API Standards User role	14
7. Permitted Users	15
7.1 Requirements of arrangements with Permitted Users	15
7.2 Third Party responsible under these Terms for acts of Permitted User	16
8. Outsourced Providers	16
9. PoC Partners	18
10. Standards Lifecycle Management	19
10.1 Managing API Standards and Operational Standards	19
10.2 Adoption of, or amendment to, Operational Standards by API Council	19
10.3 Adoption of, or amendment to, Operational Standards by the Independent Director Committee of Payments NZ	20
10.4 Chief Executive Amendment to Operational Standards	20
10.5 Notice and Expiry	20
11. Change management of Terms	21
11.1 Variation to Terms	21
12. Implementation	22
12.1 Minimum Open Banking Implementation Plan	22
12.2 API Council recommendation	22
12.3 Board of Payments NZ review	22
12.4 Publication, effective date, compliance and notification	22
12.5 Regular review	23
13. Breach	23
13.1 Notification of breach	23
13.2 Classification of breach	24
13.3 Trivial Breach procedure	24
13.4 Classification of non-Trivial Breach	25
13.5 Intermediate Breach procedure	25
13.6 Material Breach procedure	27
14. Information gathering and sharing	30
14.1 API Centre may make enquiries	30
14.2 Keeping API Centre informed of remedial steps	30
14.3 API Standard User notification	30

15.	Exemptions	30
15.1	Exemption from obligations	30
15.2	Notification and submissions	31
15.3	Exemption Application review procedure	31
15.4	Notification of decision	32
15.5	Approval of Exemption Application	32
15.6	Extension and appeal procedures	33
16.	Suspension and termination of API Standards User	34
16.1	Grounds for suspension of an API Standards User	34
16.2	Consequences of suspension	35
16.3	Application for reinstatement of Registration	35
16.4	Consideration of reinstatement by API Centre	35
16.5	Termination of an API Standards User's Registration	36
16.6	Consequences of termination	36
17.	Effect of suspension or termination	37
17.1	Survival	37
17.2	Specific effects	37
18.	Withdrawal from being an API Standards User	38
18.1	Withdrawal	38
18.2	Consequences of withdrawal	39
19.	Suspension or termination of the use of particular API Standards	40
20.	Complaints and Disputes	40
20.1	Complaints and Disputes between the API Centre and an API Standards User	40
20.2	Complaints and Disputes between Bilateral Counterparties	41
21.	Liability	41
21.1	Waiver of Liability of the API Centre to API Standards User	41
21.2	No Warranties	42
21.3	Further limitation of liability of the API Centre	42
21.4	Application of this clause to API Centre related persons and groups	42
21.5	Liability between API Standards Users	42
21.6	Cap on Liability	42
21.7	Evidence of Insurance	42
22.	Indemnity of the API Centre	43
22.1	Indemnity against External Third Party Claims	43
22.2	Indemnity from API Providers	43
22.3	Exceptions	44
22.4	Control of claims	44
23.	Key Contacts	44
24.	Ownership of Licensing and Intellectual Property Rights	45
24.1	Intellectual Property Rights	45
24.2	Licence of Brands	45
25.	Governance	45
26.	Confidentiality	46
27.	Notices	47
27.1	API Standards Users to notify any change of address	47
27.2	Address for Notices	47
27.3	Timing of receipt	47
27.4	Proof of electronic service	47

28.	General	47
28.1	Severance	47
28.2	Employees, representatives and contractors	47
28.3	Third party rights	48
28.4	No agency	48
28.5	Remedies cumulative	48
28.6	Survival	48
28.7	Entire agreement and Precedence	48
28.8	Waiver	48
28.9	Governing law and jurisdiction	48
	Appendix 1 — Registration Criteria	49
	Registration Criteria for a Third Party	49
	Registration Criteria for an API Provider	49
	Registration as an API Provider and Third Party	49
	Appendix 2 — Third Party Cap on Liability	50

API Centre Terms and Conditions

Introduction

Following extensive industry engagement, Payments NZ Limited (Payments NZ) has established the API Centre to:

- develop, maintain and publish API Standards and Operational Standards;
- promote system efficiency, security, safety and customer uptake through the use of interoperable API Standards by API Standards Users; and
- facilitate API Standards Users to gain access to Standardised APIs for them to bring their innovations to market more simply and quickly.

These Terms and Conditions set out the basis on which the API Standards are made available to API Providers and Third Parties.

1. Defined terms and interpretation

1.1 Defined terms

Except where the context otherwise requires, in these Terms:

Annual API Standards User Fee means the annual fee payable by API Standards Users which is:

- (a) set by the Board of Payments NZ from time to time in accordance with clause 5.1;
- (b) published on the API Centre's website;
- (c) payable in accordance with an invoice sent to each API Standards User; and
- (d) subject to any special arrangements agreed between Payments NZ and the API Standards User.

Application Programming Interface (API) means an application programming interface, which is a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact.

API Centre means the service established by and within Payments NZ to develop, maintain and publish API Standards and govern the use of API Standards by API Standards Users

API Centre Agreement means the agreement entered into between the API Centre and an API Standards User which binds both parties to the Terms and Conditions.

API Centre Manager means the person appointed to that position by Payments NZ and notified to the API Standards Users from time to time.

API Centre Register means the platform owned by Payments NZ and maintained by the API Centre, for use by API Standards Users in accordance with the Register Standard and Security Profile.

API Centre website means the API Centre's website located at www.apicentre.paymentsnz.co.nz (or any replacement URL from time to time) and may refer to either the Standards User only section or the public section, as specified.

API Council means the Council established by Payments NZ to govern the development, maintenance, and publication of API Standards by the API Centre and the use of API Standards by API Standards Users.

API Council Charter means the governance charter adopted by the Board of Payments NZ setting out the governance protocols and policies of the API Council and the Independent Committee.

API Provider means a person who is registered by the API Centre as an API Provider.

API Standards means the API standards developed, maintained, and published by the API Centre.

API Standards User means an API Provider or a Third Party whose application for registration as an API Standards User has been approved in accordance with these Terms and who has entered into the API Centre Agreement.

Bilateral Agreement means any agreement between an API Provider and a Third Party the subject matter of which is, or includes, access to and use of Standardised APIs.

Bilateral Counterparty means, in relation to an API Standards User, another API Standards User with whom the first API Standards User has entered into a Bilateral Agreement.

Business Day means any day other than a Saturday or Sunday or public holiday (as that term is defined in the Holidays Act 2003, but excluding provincial anniversary days).

Chief Executive means the Chief Executive of Payments NZ.

Company Staff means the Chief Executive and any other Payments NZ staff who have been delegated authority by the Board of Payments NZ to exercise functions or powers in respect of the API Centre.

Compliance Standard means the Operational Standard relating to compliance requirements for API Standards Users, as amended from time to time.

Confidential Information means information or material of a confidential nature belonging or relating to a party, or information or material relating to a natural person and which is in a party's control, in whatever form (whether tangible and/or visible or not), that is disclosed or communicated by a party to the other party, or to another person, or learnt or accessed by the other party by whatever means, in connection with an API Centre Agreement, but for the avoidance of doubt, does not include these Terms.

Customer, in respect of an API Provider, means a person who holds an account with that API Provider.

Customer Consent means either a Customer Data Consent or a Customer Payment Consent, as applicable.

Customer Data means:

- (a) information about a Customer, or their account with an API Provider, which is available through a Standardised API, including information used in the processing or facilitation of a payment or other transaction; but
- (b) does not include data which has been provided pursuant to a Customer Consent and which has subsequently been shared with another party under a separate customer consent pursuant to clause 2.7(b) of the Customer Standard from the relevant Customer only to the extent it has been shared under that separate customer consent.

Customer Data Breach means disclosure of the following information or data to a third party who is not authorised to receive it:

- (a) information or data acquired through a Standardised API;
- (b) information or data created as an outcome of the use of a Standardised API.

For the avoidance of doubt, information or data includes, without limit, Customer Data.

Customer Data Consent means consent given by a Customer to an API Provider, a Third Party or a PoC Partner that meets the requirements of the Customer Standard, under which the Customer authorises:

- (a) the Third Party or PoC Partner to contact the Customer's API Provider to request Customer Data;
- (b) the transfer of their Customer Data through a Standardised API;
- (c) the use of the Customer Data by the nominated party(s) for the agreed purpose; and
- (d) the API Provider to act on an instruction received from a Third Party or PoC Partner in relation to Customer Data.

Customer Payment Consent means the consent given by a Customer to the API Provider, Third Party or a PoC Partner that meets the requirements of the Customer Standard, under which the Customer authorises:

- (a) an enduring payment or a payment under which funds will be debited from the Customer's account and credited to the beneficiary nominated in the Customer Payment Consent;
- (b) the Third Party or PoC Partner to contact the Customer's API Provider; and
- (c) the API Provider to act on an instruction received from a Third Party or PoC Partner, on behalf of the Customer in respect of that payment transaction.

Customer Related Service means a service provided to a Customer by a Third Party by means of a Standardised API.

Customer Standard means the Operational Standard relating to access, use, disclosure, and authorities for Customer payment transactions, as amended from time to time.

Data Security Standard means the Operational Standard relating to the protection of information and data provided to, or obtained by, an API Standards User and processes for managing unauthorised use or disclosure, as amended from time to time.

Effective Date means the date on which the Terms and Conditions are binding on an API Standards User pursuant to an API Centre Agreement.

Exemption Application means the application described in clause 15.1(a).

Force Majeure Event means:

- (a) an act of God such as an earthquake, flood, volcanic activity or other natural disaster;
- (b) fire, epidemic, riot, terrorism or war;
- (c) a lock-out, strike or other industrial dispute;
- (d) an act or omission by a government agency; or
- (e) any other event or circumstance ("event") of a similar nature, that is beyond the reasonable control of the affected party,

but excludes:

- (f) an event where the event, or the effect of the event on the affected party, could have been avoided or overcome by the affected party taking reasonable precautions;

- (g) a lock-out, strike or other industrial dispute that relates solely to the affected party's or its related companies' (as defined in section 2(3) of the Companies Act 1993 except that "company" shall mean a company or other body corporate wherever incorporated) workforce;
- (h) the failure of a contractor or supplier, except to the extent such failure is itself caused by a Force Majeure Event; or
- (i) a lack of funds for any reason.

GST means goods and services tax chargeable, or to which a person may be liable, under the GST Act at the rate prevailing from time to time, including any tax levied in substitution for that tax.

GST Act means the Goods and Services Tax Act 1985.

Independent Committee means the independent committee of the API Council, comprising individuals with relevant industry expertise appointed by Payments NZ who are independent of any API Standards User.

Independent Director Committee of Payments NZ means the independent committee of the Board of Payments NZ Limited, comprising the Independent Directors of Payments NZ.

Independent Director of Payments NZ means a director of Payments NZ Limited of the Payments NZ Limited constitution.

Industry Sandbox means a website and testing environment provided and maintained by the API Centre where API Standards Users can connect to and test applications and services that use the Standardised APIs.

Insolvency Event means in relation to an API Standards User, that any of the following occur:

- (a) the API Standards User is put into liquidation;
- (b) the API Standards User ceases or threatens to cease to carry on most or all of its business or operations;
- (c) an application is made or proceedings are issued for a court order and in either case not withdrawn, stayed or dismissed within 10 Business Days, or an order is made, or an effective resolution is passed, or any action of a similar nature is taken, for the dissolution or reorganisation of the API Standards User, except for the purpose of a solvent reconstruction, merger or voluntary liquidation previously approved in writing by the API Centre (such approval not to be unreasonably withheld);
- (d) the API Standards User makes or proposes to make any assignment, arrangement, compromise or composition with, or for the benefit of, any of its creditors;
- (e) a receiver, trustee, manager, administrator (including a voluntary administrator appointed under Part 15A of the Companies Act) or similar officer is appointed in relation to an API Standards User;
- (f) a receiver, trustee, manager, administrator (including a voluntary administrator appointed under Part 15A of the Companies Act) or similar officer is appointed in relation to all or a substantial part of the API Standards User's assets; or
- (g) anything analogous or having substantially similar effect occurs under the law of any applicable jurisdiction in relation to the API Standards User,

and to become insolvent has a corresponding meaning.

Intellectual Property means all rights and interests (including common law rights and interests) in any patents, patent applications, trademarks, trade, business, domain or company names, logos, registered designs, design rights, copyright, moral rights, database

rights, know-how, trade secrets, domain names, internet addresses, rights in confidential information, all and any other intellectual or industrial rights, whether registered or unregistered, and all rights or forms of protection of a similar nature or having equivalent or similar effect to any of these that may subsist anywhere in the world.

Intermediate Breach means any breach of these Terms that is not a Trivial Breach but does not meet the threshold of a Material Breach.

Key Contact means each person nominated by an API Standards User from time to time as its primary point of contact in relation to its use of the API Standards.

Major Version means, in relation to any API Standard, an iteration of that API Standard where significant changes are made or significant new features are introduced.

Material Breach means any breach of these Terms which has, or is likely to have, a significant and detrimental impact on the API Centre, the API Centre Register, an API Standards User, a Standardised API or any Customer's interests, and shall be deemed to include, but is not limited to, the following:

- (a) using the API Standards for any illegal or improper purpose in a way that violates any law or violates, infringes or misappropriates any rights of a third party;
- (b) a breach of any security measure prescribed by the API Standards or the Operational Standards;
- (c) a Persistent Breach of these Terms;
- (d) any failure to pay the applicable annual API Standards User fees when those fees are due after a notice of default has been served on the API Standards User and it has failed to make payment in the period specified in that notice; or
- (e) an act or omission that causes, or is likely to cause, a Material Risk Event.

Material Risk Event means any event that poses a material risk to:

- (a) the integrity, security and efficiency of any of the following:
 - (i) the API Centre;
 - (ii) the API Centre Register;
 - (iii) an API Standards User;
 - (iv) a Standardised API; or
- (b) a Customer or their interests.

Minimum Open Banking Implementation Plan means a plan published from time to time in accordance with clause 12 (and includes an amendment to an existing Minimum Open Banking Implementation Plan) which sets out the minimum requirements an API Provider must meet in relation to the implementation of a Standardised API to ensure that a Standardised API is technically and operationally ready for use with Third Parties, including details relating to:

- (a) when an API Provider must implement and be technically and operationally capable of making a Standardised API available to Third Parties; and
- (b) any other minimum requirements the API Council deems necessary, including but not limited to:
 - (i) the version and description of the Standardised API;
 - (ii) the functional scope, account types and customer eligibility; and

- (iii) requirements which are intended to ensure that, by the date or dates specified in the plan, the API Provider:
 - (A) has completed all technical testing of the Standardised API;
 - (B) is able to connect with Third Parties using the Standardised API;
 - (C) has business structures in place so that it can enter into arrangements with Third Parties to use the Standardised API; and
 - (D) has all necessary structures and processes in place to use the Standardised API with Third Parties.

Operational Standards means the operational standards developed, maintained, and published on the API Centre website applicable to API Standards Users in relation to their compliance obligations as API Standards Users, or the implementation or use of Standardised APIs.

Outsourced Provider means a third party services provider who is not an API Standards User but who provides services to an API Standards User using Standardised APIs for the exclusive benefit of that API Standards User in accordance with clause 8.

Permitted User means a person who:

- (a) has a direct contractual relationship with a Customer; and
- (b) has an arrangement with a Third Party or a PoC Partner which enables that person to instruct a Third Party to, in a manner permitted by a Customer Consent:
 - (i) share Customer Data in order to provide services to that Customer; or
 - (ii) initiate a payment on behalf of that Customer; and
- (c) initiates the collection of a Customer Consent through its own interface or application.

Persistent Breach means when an API Standards User:

- (d) breaches obligations contained in these Terms on multiple occasions over a period of time, whether or not the individual breaches are Trivial Breaches; or
- (e) continues to breach an obligation contained in these Terms for an extended period of time and fails to remedy that breach or obtain an exemption where required to do so in accordance with these Terms.

PoC Partner means a person who is conducting a Proof of Concept with an API Provider.

Proof of Concept means a test-and-learn partnering experience where a PoC Partner conducts testing of a business proposition in a live and/or non-production environment involving Customers of the API Provider using the Standardised APIs with a PoC Partner in accordance with the requirements set out in clause 9.

Register User Account means the user account set up for each API Standards User in the API Centre Register by the API Centre in accordance with the Register Standard.

Registration means:

- (a) the process undertaken by the API Centre to register a person as an API Standards User where that person demonstrates that it satisfies the Registration Criteria and the requirements of these Terms; and
- (b) in relation to an API Standards User, that person's designation as a API Standards User after completion of the above process.

Registration Criteria means the criteria required to be met in order to be registered as an API Standards User as set out in Appendix 1.

Register Standard means the Operational Standard relating to the provision, maintenance, and use of the API Centre Register, as amended from time to time.

Related Entity means a related company under the Companies Act 1993 or a related body corporate provided that any reference in the Companies Act 1993 to a “company” is deemed to include any partnership, body corporate, association or other entity, whether incorporated or unincorporated, irrespective of the place of incorporation or registration of that partnership, body corporate, association or other entity.

Relevant Law means in respect of an API Standards User and the API Centre, all laws and regulations relevant in performing the obligations or claiming any rights of that party under these Terms and in carrying on that party’s business, including:

- (a) the Privacy Act 2020;
- (b) the Financial Service Providers (Registration and Dispute Resolution) Act 2008;
- (c) the Financial Markets Conduct Act 2013;
- (d) the Anti-Money Laundering and Countering Financing of Terrorism Act 2009;
- (e) the Fair Trading Act 1986;
- (f) the Consumer Guarantees Act 1993;
- (g) the Commerce Act 1986;
- (h) the Secret Commissions Act 1910; and
- (i) any notice, guideline, order or ruling made pursuant to Relevant Law or regulation.

Reporting Standard means the Operational Standard relating to obligation to report information about use of API Standards, as amended from time to time.

Security Profile means the security profile published on the API Centre website which defines how API Standards Users will securely and safely interact with Standardised APIs, as amended from time to time.

Standardised API means any API developed or used by an API Standards User that complies with the API Standards, but does not include any enhanced functionality added to the Standardised API.

Standards Lifecycle Management Policy means the policy adopted and maintained by the API Centre to manage the versioning and lifecycle management of API Standards, as approved by the API Council.

Suspension has the meaning set out in clause 17 of these Terms.

Technical Service Provider means a party identified in the Key Commercial Details of a Bilateral Agreement (as replaced time to time) that operates the Standardised API connections and flows on behalf of the Third Party.

Terms and Conditions (or Terms) means the terms and conditions of being an API Standards User including the appendices (as updated from time to time and published on the API Centre website) and referred to as Terms.

Template Bilateral Agreement means a template bilateral agreement provided and maintained by the API Centre available to API Standards Users when entering into Bilateral Agreements (as updated from time to time and published on the Standards User only section of the API Centre website).

Third Party means a person who is an API Standards User that is registered by the API Centre as a Third Party.

Trivial Breach means any breach of these Terms which has a negligible impact on the API Centre, the API Centre Register, any API Standards User, a Standardised API or a Customer's interests.

Unauthorised Use means any use of the API Standards or a Standardised API that is:

- (a) not authorised by a Customer (if the Customer's authorisation is required); or
- (b) otherwise in breach of the Terms and Conditions.

Virus means malware or other software designed to modify, damage, destroy, record or transmit information within a computer, computer system, API or network without the permission of the owner, including computer viruses, backdoor software, time bombs, Trojan horses, worms, drop dead devices or similar items.

1.2 Legal Parties

(a) In this Agreement:

- (i) a reference to the "API Centre" is a reference to Payments NZ in its capacity as the provider of the API Centre;
- (ii) a reference to the "API Council" is a reference to Payments NZ performing its functions through that body, under the terms of the API Council Charter; and
- (iii) a reference to the "Independent Committee" is a reference to that committee performing its functions under the API Council Charter.

(b) The API Council, the Independent Committee and Company Staff will assist the API Centre in carrying out its functions under these Terms in accordance with the delegated authorities of the Board of Payments NZ.

1.3 Interpretation

In these Terms, unless the context otherwise requires:

- (a) appendix and other headings are for ease of reference only and will not affect the interpretation of these Terms;
- (b) references to clauses or appendices are references to clauses or appendices of these Terms;
- (c) words importing the singular include the plural and vice versa;
- (d) references to "including" and similar expressions are not limited by specific examples;
- (e) derivations of any defined word or term will have a corresponding meaning;
- (f) a document (however described and including these Terms) includes that document as amended or replaced from time to time;
- (g) an obligation not to do something includes an obligation not to allow or cause that thing to be done;
- (h) any reference to a statute includes references to regulations, orders or notices made under or pursuant to such statute, and amendments to that statute, and a statute or regulation passed in substitution for the statute;
- (i) references to a "person" (other than a natural person) includes a firm, a body corporate, a partnership, a joint venture, an unincorporated body or association, or any government agency or authority;

- (j) a reference to a person includes a reference to the person's executors, administrators, successors, substitutes (including persons taking by novation) and assignees; and
- (k) a requirement that information be in writing is met by information that is in electronic form if the information is readily accessible so as to be usable for subsequent reference.

2. Application of Terms

- (a) These Terms will apply to each API Standards User from the Effective Date.
- (b) The API Centre may, amend these Terms at any time in accordance with clause 11 of these Terms.

3. Registration of API Standards Users

- (a) To apply to become an API Standards User an applicant must demonstrate that it meets the Registration Criteria set out in Appendix 1 and complete the application form on the Standards User only section of the API Centre website.
- (b) An applicant must provide all supporting information requested by the API Centre in relation to its application and warrants and represents that the information and documentation provided in, or accompanying, its application form for Registration, is true, complete, and correct in all material respects and that all information and documentation relevant to the application process has been disclosed to the API Centre.
- (c) The Chief Executive of Payments NZ will, in accordance with these Terms, determine applications for Registration of API Standards Users.
- (d) The API Centre will notify the applicant of the decision of the Chief Executive of Payments NZ as soon as practicable after the determination has been made.
- (e) If the Chief Executive of Payments NZ approves an application for Registration of an API Standards User:
 - (i) the applicant will enter into the API Centre Agreement with the API Centre and will be bound by these Terms;
 - (ii) the API Centre will enter the applicant's details on the register of API Standards Users and Key Contacts;
 - (iii) the API Centre will enter the applicant's details into the API Centre Register; and,
 - (iv) the applicant will be registered as an API Standards User from the Effective Date.

4. API Centre role

4.1 The API Centre will, in accordance with these Terms:

- (a) create, maintain, amend and publish API Standards and any associated documentation;

- (b) create, maintain, amend and publish Operational Standards and any associated documentation;
- (c) authorise (and hereby authorises) each API Standards User to use the API Standards for the purpose, and on the terms, set out in these Terms;
- (d) govern the use of API Standards and Operational Standards by API Standards Users;
- (e) monitor, through the annual attestation process set out in clause 17, compliance by API Standards Users with these Terms;
- (f) manage the breach, suspension, and termination processes in relation to an API Standards User;
- (g) regularly review these Terms for their adequacy to promote the integrity, security and efficiency of API Standards developed and maintained by the API Centre and used by API Providers and Third Parties;
- (h) update these Terms as the API Centre considers is required;
- (i) set and amend the Annual API Standards User Fee in accordance with clause 5.1 of these Terms;
- (j) maintain the register of API Standards Users and Key Contacts;
- (k) maintain a confidential register of Bilateral Agreements entered into between API Standards Users to enable the API Centre to notify a Bilateral Counterparty where it is required to do so under these Terms, such register to only record the existence of the Bilateral Agreements and not the terms of the Bilateral Agreements;
- (l) consider any Bilateral Agreement dispute referred by API Standards Users in accordance with the dispute resolution process in these Terms;
- (m) notify risk events to affected API Standards Users by informing them as soon as reasonably practicable after it becomes aware of the risk event, including:
 - (i) viruses, malware, or other harmful code and DOS/DDOS or such attacks affecting API Standards Users; or
 - (ii) an Insolvency Event in respect of an API Standards User; or
 - (iii) a Material Risk Event;
- (n) maintain a Template Bilateral Agreement and publish updated versions on the Standards User only section of the API Centre website;
- (o) provide and maintain, an Industry Sandbox, an API Centre Register, Confluence wiki, GitHub repository, and website;
- (p) provide operational, administrative and record-keeping support in respect of the API Centre Agreement, the API Standards, Standardised APIs and Operational Standards; and
- (q) comply with Relevant Law in relation to its obligations under these Terms.

4.2 The API Centre may, in accordance with these Terms:

- (a) maintain a confidential register of Permitted Users, Outsourced Providers and PoC Partners; and
- (b) for the purpose stated in sub-clause (a), obtain from API Standards Users any information the API Centre may reasonably request in relation to Permitted Users,

Outsourced Providers and PoC Partners that an API Standards User is using Standardised APIs with.

5. Setting the Annual API Standards User Fee

5.1 Board will set Annual API Standards User Fee

- (a) The Board of Payments NZ will set and amend the Annual API Standards User Fee from time to time.
- (b) In setting or amending the Annual API Standards User Fee, the Board must:
 - (i) ensure that it has received a recommendation from the Independent Committee and have regard to that recommendation; and
 - (ii) be satisfied that the proposed Annual API Standards User Fee is in the best interests of the API Centre and enables the API Centre to deliver the approved annual work plan.

6. API Standards User role

Each API Standards User must, in accordance with these Terms:

- (a) comply with the API Centre Agreement;
- (b) ensure that each Standardised API which it uses complies with, and is used in accordance with, the API Standards;
- (c) comply with the Operational Standards in relation to their compliance obligations as API Standards Users, and in relation to the implementation, and all uses of, Standardised APIs;
- (d) undertake testing of each Standardised API to ensure that its use of the Standardised API is in accordance with these Terms or the terms of any Bilateral Agreement, prior to the use of that Standardised API;
- (e) ensure that the API Standards are used only with:
 - (i) another API Standards User;
 - (ii) any Permitted Users in accordance with clause 7;
 - (ii) any Outsourced Providers in accordance with clause 8; and
 - (iii) any PoC Partners who are conducting a Proof of Concept in accordance with clause 9;
- (f) maintain its status as an API Standards User at all times during the term of any Bilateral Agreement entered into with another API Standards User relating to use of Standardised APIs;
- (g) ensure that any Bilateral Agreement entered into by it is consistent with, and gives effect to, these Terms, including the requirements in clauses 15 to 19 in relation to suspension, termination or withdrawal;
- (h) notify the API Centre of any Bilateral Agreement which it enters into with another API Standards User and if that Bilateral Agreement expires or is terminated, so that the API Centre can maintain a confidential register of Bilateral Agreements for the purposes set out in these Terms;

- (i) pay the applicable annual API Standards User fees (plus GST) to Payments NZ as invoiced by Payments NZ, when those fees are due;
- (j) comply with Relevant Law in relation to its use of the API Standards and Standardised APIs;
- (k) act in a way that maintains the integrity, security and efficiency of the API Centre;
- (l) at all times, continue to comply with the Registration Criteria;
- (m) continue to obtain or hold (as the context requires) the relevant Customer Consents in accordance with the relevant API Standards and Operational Standards; and
- (n) as soon as reasonably practicable, notify the API Centre of:
 - (i) any adverse material change in circumstances which may affect that API Standards User's ability to satisfy the Registration Criteria or any matter under its API Centre Agreement or any Bilateral Agreement that is likely to, or does, undermine the integrity, security and efficiency of the API Centre or the API Standards;
 - (ii) any Unauthorised Use or Customer Data Breach in accordance with the Data Security Standard; or
 - (iii) any possible breach of the API Centre Agreement (including these Terms) in the manner set out at clause 17.

7. Permitted Users

7.1 Requirements of arrangements with Permitted Users

A Third Party who enters into an arrangement with a Permitted User under which the Third Party provides that Permitted User with access to Customer Data or the ability to initiate a payment on behalf of a Customer using a Standardised API must ensure that:

- (a) the arrangement complies with all Relevant Laws, these Terms and Conditions (including in relation to Customer Consents) and any Bilateral Agreement entered into with another API Standards User;
- (b) the terms of use that apply as between the Customer and the Permitted User in respect of the Permitted User's services include:
 - (i) a binding obligation on the Permitted User not to access, use or disclose Customer Data in a manner that would cause the Third Party to be in breach of clause 7.2;
 - (ii) a clear statement that the Permitted User will be responsible to the Customer for the Permitted User's own acts and omissions in relation to any Customer Data provided to, or payment transaction initiated on the instruction of, the Permitted User through the use of the Standardised API, including any breach by the Permitted User of the obligation described in (i) above; and
 - (iii) details of where the Customer can access the Third Party's dispute resolution process that it has, and makes publicly available, in accordance with clause 3.2 of the Customer Standard; and
- (c) the Third Party imposes legally-binding obligations on the Permitted User that require the Permitted User:
 - (i) to immediately notify the Third Party in the event that the Permitted User becomes aware of any access, disclosure, or use of Customer Data by the

Permitted User that is not in accordance with an express consent given by the relevant Customer;

- (ii) to take all steps reasonably available to the Permitted User to co-operate with and assist the Third Party to comply with its obligations under clauses 3.10 and 3.11 of the Data Security Standard or clause 13 of these Terms; and
- (iii) to comply with the terms of any suspension, termination, or any additional conditions relating to the Permitted User's use of the Standardised API or access to Customer Data as advised by the Third Party in the event that the Third Party is directed by the API Centre to impose such suspension, termination, or conditions in accordance with clause 13.6 of these Terms;
- (iv) if requested by the Customer, to delete, destroy or anonymise the relevant Customer Data (except to the extent that any Customer Data must be retained by a law or relates to any current or anticipated legal proceedings or dispute resolution proceedings); and
- (v) to provide the Customer with clear, conspicuous mechanisms to expressly grant consent to the Permitted User for any proposed use or disclosure by the Permitted User of any Customer Data in a manner not permitted by the Customer Consent under which the Customer Data was initially disclosed to the Permitted User, which must, at a minimum, include:
 - (A) a description of the data it applies to;
 - (B) the details of the persons that the data will be disclosed to (if any);
 - (C) duration of consent and confirmation it can be revoked (if applicable); and
 - (D) the purpose for which it will be used or disclosed.
- (d) the Permitted User has in place security measures that are no less onerous on the Permitted User, or protective of the interests of the Customer, than those described in clause 2.2 of the Data Security Standard, and the Permitted User will otherwise do all things reasonably necessary to allow the Third Party to fully comply with its obligations under sections 2 to 3 of the Data Security Standard.

7.2 Third Party responsible under these Terms for acts of Permitted User

A Third Party who enters into an arrangement with a Permitted User is responsible, under these Terms, for ensuring that no access, use or disclosure of such Customer Data by that Permitted User occurs other than in accordance with:

- (a) the relevant Customer Consent; or
- (b) any express consent regarding access, use or disclosure of that Customer Data that the Permitted User has collected from the Customer in accordance with clause 7.1(c)(v).

Any such unauthorised access, use, or disclosure by the Permitted User will constitute a breach of these Terms by the relevant Third Party.

8. Outsourced Providers

- (a) Subject to the conditions in sub-clause (b) and sub-clause (d), use of Standardised APIs is allowed in circumstances where an API Standards User uses the Standardised APIs to exchange data, including Confidential Information and Customer Data (together, the Transferred Data) with an Outsourced Provider where:

- (i) the contractual terms of the service agreement between the API Standards User and the Outsourced Provider provide that the Outsourced Provider uses the Standardised APIs and receives, accesses, stores, uses and discloses the Transferred Data solely for the purpose of providing a service to the API Standards User; and
 - (ii) the API Standards User exclusively benefits from the arrangements between it and the Outsourced Provider for the use of the Standardised APIs and exchange of the Transferred Data in a processed or otherwise improved format from the Outsourced Provider.
- (b) The following conditions must be met for sub-clause (a) to apply:
- (i) access, receipt, storage, use and disclosure of any Customer Data contained in the Transferred Data by the Outsourced Provider is:
 - (A) disclosed by the API Standards User to the Customer; and
 - (B) included in the Customer Data Consent,
 in accordance with the API Standards User's obligations under the Privacy Act 2020;
 - (ii) the API Standards User is accountable and liable to the Customer (and may not seek to contract out of such liability with the Customer) for the acts and omissions of the Outsourced Provider in relation to any Transferred Data provided through the use of a Standardised API; and
 - (iii) the API Standards User must impose the following legally binding obligations on the Outsourced Provider:
 - (A) the Outsourced Provider must access, receive, store, use and disclose the Transferred Data it receives through the use of Standardised APIs in accordance with the purposes stated in sub-section (a);
 - (B) the Outsourced Provider must be prohibited from accessing, receiving, storing, using or disclosing any Transferred Data for any of its own purposes except for providing the API Standards User with a service;
 - (C) the Outsourced Provider must access, receive, store, use, disclose and delete or anonymise all Transferred Data in a manner that complies with all Relevant Laws, the API Centre Agreement and any Bilateral Agreement that the API Standards User has entered into; and
 - (D) the Outsourced Provider must have comparable security obligations that are of a standard equal to or better than those under the Data Security Standard.
- (c) For the avoidance of doubt, an Outsourced Provider who uses the Standardised APIs to exchange Transferred Data with an API Standards User does not need to apply to register as a Third Party, unless, subject to sub-clause (d) the Transferred Data and the Standardised APIs are used for the Outsourced Provider's own benefit (including offering new or improved products or services to customers of the Outsourced Provider's who are not API Standards Users , and/or connecting with another API Standards User for any other purpose other than for the purposes described in sub-clause 8(a)).
- (d) If an Outsourced Provider becomes a PoC Partner, sub-clauses 8(b)(iii)(A)-(C):
- (i) continue to apply to the Outsourced Provider's activities that relate to its functions as an Outsourced Provider; but

- (ii) do not apply to the Outsourced Provider's activities that relate to its Proof of Concept for the duration of the Proof of Concept in accordance with clause 9.

9. PoC Partners

- (a) Subject to the conditions in sub-clauses (b) and (c), an API Provider may use the Standardised APIs with a PoC Partner for the sole purpose of conducting a Proof of Concept.
- (b) The following conditions must be met for sub-clause (a) to apply:
 - (i) the commencement and conclusion dates of the Proof of Concept and a description of each PoC Partner must be notified to the API Centre by the API Provider prior to the commencement of each Proof of Concept
 - (ii) the duration of each Proof of Concept between the API Provider and each PoC Partner must not exceed 12 months;
 - (iii) the aggregate number of mutual Customers of the API Provider and the PoC Partner that are included in each Proof of Concept must not exceed 1,000;
 - (iv) the API Provider must act in accordance with a Customer Consent to provide the PoC Partner with any access to Customer Data and/or the ability to initiate a payment on behalf of the Customer; and
 - (v) the API Provider must impose legally binding obligations on the PoC Partner
 - (A) that are no less onerous on the PoC Partner or no less protective of the interests of the Customer than:
 - (I) the security measures in accordance with the Data Security Standard;
 - (II) the Customer Consent requirements as they apply to Third Parties in accordance with the Customer Standard; and
 - (III) the requirements for entering into an arrangement with a Permitted User as they apply to Third Parties in accordance with clause 7 of these Terms and the Customer Standard; and
 - (B) the API Provider must impose a legally binding obligation on each PoC Partner that the PoC Partner must use the Standardised APIs:
 - (A) in the case of a PoC Partner that is also a Permitted User or Outsourced Provider, for the sole purposes of:
 - (I) conducting the Proof of Concept and
 - (II) any other use in accordance with that PoC Partner's function as a Permitted User or Outsourced Provider; and
 - (B) in the case of any other PoC Partner, for the sole purpose of conducting the Proof of Concept.
- (c) The API Centre may request information from an API Provider relating to a prospective, current or past Proof of Concept or PoC Partner for the purpose of understanding and improving the API Centre's Proof of Concept framework.

10. Standards Lifecycle Management

10.1 Managing API Standards and Operational Standards

The API Centre is responsible for creating, maintaining and publishing API Standards and Operational Standards. The API Council carries out these functions on behalf of the API Centre and, when doing so will:

- (a) consult with API Standards Users, except in the case of API Standards if the Standards Lifecycle Management Policy permits otherwise;
- (b) allow API Standards Users to provide feedback within a timeframe specified by the API Council, except in the case of API Standards if the Standards Lifecycle Management Policy permits otherwise;
- (c) consider feedback provided;
- (d) in relation to API Standards:
 - (i) ensure that any change, Major Version release or other update to an API Standard does not detrimentally affect the operation of the affected Standardised APIs and that any such change, Major Version release or other update is, at a minimum, backwards compatible with n-1 versions of the affected Standardised APIs; and
 - (ii) give API Standards Users reasonable notice, in the circumstances, in relation to any material change, Major Version release or other update to an API Standard.

10.2 Adoption of, or amendment to, Operational Standards by API Council

- (a) The API Council, in consultation with API Standards Users, may adopt or amend an Operational Standard at any time in accordance with the following process:
 - (i) notice of the proposed adoption of, or amendment to, the Operational Standard must be given to the Independent Director Committee of Payments NZ;
 - (ii) the Independent Director Committee of Payments NZ must, as soon as practicable, confirm whether it wishes to object to the proposed adoption of, or amendment to, the Operational Standard;
 - (iii) in making a decision on whether it wishes to object to the proposed adoption of, or amendment to, the Operational Standard, the Independent Director Committee of Payments NZ must have regard to the API Council objectives and the constitutional objectives of Payments NZ Limited;
 - (iv) if a majority of the Independent Director Committee of Payments NZ object to the adoption of, or amendment to, the Operational Standard, the Independent Director Committee of Payments NZ must advise the API Council as soon as practicable and the proposed adoption of, or amendment to, the Operational Standard will be of void and of no effect;
 - (v) if the Independent Director Committee of Payments NZ does not object to the proposed adoption of, or amendment to, the Operational Standard in accordance with clause 10.2(a)(iv), it must advise the API Council as soon as practicable;
 - (vi) the API Council must give API Standards Users reasonable notice, in the circumstances, that the Operational Standard has been adopted or amended following receipt of a notice of no objection in accordance with clause

10.2(a)(v). Except where the API Council reasonably considers that an urgent adoption of, or amendment to, the Operational Standard is required, the API Centre will give API Standards Users not less than 40 Business Days' notice prior to publication of the Operational Standard.

- (b) Each API Standards User acknowledges and agrees that, by entering into the API Centre Agreement, it will be bound by any Operational Standard from the effective date specified in the notice given under clause 10.2(a)(vi) above.

10.3 Adoption of, or amendment to, Operational Standards by the Independent Director Committee of Payments NZ

- (a) An Operational Standard may be adopted or amended at any time by a majority of the Independent Director Committee of Payments NZ, in consultation with the API Council, provided that:
 - (i) the Independent Director Committee of Payments NZ considers such adoption or amendment is necessary or desirable to promote the integrity, safety, security and efficiency of the API Centre or the integrity, safety, security and efficiency of Standardised APIs; and
 - (ii) API Standards Users are given reasonable notice, in the circumstances, of the adoption or amendment to an Operational Standard. Except where the Independent Director Committee of Payments NZ reasonably considers that an urgent adoption of an Operational Standard or amendment to an Operational Standard is required, the API Centre will give API Standards Users not less than 40 Business Days' notice prior to publication of the Operational Standard.
- (b) Each API Standards User acknowledges and agrees that, by entering into the API Centre Agreement, it will be bound by any Operational Standard from the effective date specified in the notice given under clause 10.3(a)(ii) above.

10.4 Chief Executive Amendment to Operational Standards

- (a) An Operational Standard may be amended by the Chief Executive of Payments NZ, if, in the opinion of the Chief Executive of Payments NZ, the amendment is:
 - (i) to correct a manifest error; or
 - (ii) is of a grammatical, formatting, typographical or minor nature,(each such amendment being a Chief Executive Amendment).
- (b) The API Centre must give written notice of each Chief Executive Amendment (a Chief Executive Amendment Notice) to each API Standards User no later than five Business Days after the date that the Chief Executive Amendment is made.
- (c) Except with the consent of each API Standards User, no Chief Executive Amendment may take effect earlier than 40 Business Days from the date of the Chief Executive Amendment Notice.
- (d) Each API Standards User acknowledges and agrees that, by entering into the API Centre Agreement, it will be bound by any Operational Standard from the effective date specified in the notice given under clause 10.4(c) above.

10.5 Notice and Expiry

- (a) The API Centre will notify API Standards Users of:

- (i) any material change, Major Version release or other update to an API Standard and the date on which this comes into effect by publishing details on its website;
 - (ii) any change to an Operational Standard and the date on which this comes into effect by publishing details on its website, unless such change is a Chief Executive Amendment (in which case clause 10.4 applies); and
 - (iii) any new API Standard or Operational Standard and the date on which this comes into effect by publishing details on its website.
- (b) The API Centre will use reasonable endeavours to give API Standards Users not less than 6 months prior notice of the date an API Standard (or a version of an API Standard) is to expire, by publishing details of that expiry on its website and sending a notice to API Standards Users.
- (c) Where an API Standard (or a version of an API Standard) has expired, each API Standards User must cease using that API Standard (or that version of that API Standard) on and from the expiry date, but for the avoidance of doubt, if Bilateral Counterparties wish to use an expired API Standard (or that version of that API Standard) for the purposes of an API outside the bounds of these Terms, they may continue to do so, but:
- (i) must ensure that that API is not held out or represented to be a Standardised API; and
 - (ii) the use of that API will not be covered under these Terms.

11. Change management of Terms

11.1 Variation to Terms

- (a) The Board of Payments NZ may, in consultation with the API Council, amend these Terms at any time, if it considers an amendment is necessary or desirable to promote the integrity, security and efficiency of the API Centre or the integrity, security and efficiency of Standardised APIs.
- (b) The API Council, in consultation with API Standards Users, may make a recommendation to the Board of Payments NZ to amend these Terms at any time, if it considers an amendment is necessary or desirable to promote the integrity, security and efficiency of the API Centre or the integrity, security and efficiency of Standardised APIs.
- (c) If the Board of Payments NZ amends the Terms, the effective date of the amended Terms will be the date on which the API Centre publishes the amended Terms on its website.
- (d) The API Centre will notify API Standards Users that the Terms have been amended and the effective date of the amended Terms. Except where the Board of Payments NZ reasonably considers that an urgent amendment to the Terms is required, the API Centre will give API Standards Users not less than 40 Business Days' notice prior to publication.
- (e) Each API Standards User acknowledges and agrees that, by entering into the API Centre Agreement, it will be bound by any amended Terms from the date they are published on the Standards User only section of the API Centre website.

12. Implementation

12.1 Minimum Open Banking Implementation Plan

The API Council may, at any time, recommend to the Board of Payments NZ:

- (a) the publication of a Minimum Open Banking Implementation Plan; or
- (b) the publication of one or more amendments to an existing Minimum Open Banking Implementation Plan.

12.2 API Council recommendation

Before making a recommendation under clause 12.1, the API Council must consult with all API Standards Users and must be satisfied that the Minimum Open Banking Implementation Plan will:

- (a) promote system efficiency, security, safety and customer uptake through the use of interoperable API Standards by API Standards Users;
- (b) facilitate API Standards Users to gain access to Standardised APIs for them to bring their innovations to market more effectively and efficiently; and
- (c) specify implementation requirements (including timeframes) that are reasonable for API Providers to meet.

12.3 Board of Payments NZ review

- (a) The Board of Payments NZ will review the recommendation of the API Council under clause 12.2 as soon as practicable after the recommendation is given and will either:
 - (i) approve the proposed Minimum Open Banking Implementation Plan;
 - (ii) approve the proposed Minimum Open Banking Implementation Plan subject to any changes the Board of Payments NZ, acting reasonably, considers appropriate; or
 - (iii) decide not to approve the proposed Minimum Open Banking Implementation Plan.
- (b) If the Board of Payments NZ decides to approve the proposed Minimum Open Banking Implementation Plan in accordance with subclause (a), it must be satisfied that the Minimum Open Banking Implementation Plan will:
 - (i) promote system efficiency, security, safety and customer uptake through the use of interoperable API Standards by API Standards Users;
 - (ii) facilitate API Standards Users to gain access to Standardised APIs for them to bring their innovations to market more effectively and efficiently; and
 - (iii) specify implementation requirements (including timeframes) that are reasonable for API Providers to meet.

12.4 Publication, effective date, compliance and notification

- (a) Notification: Where a Minimum Open Banking Implementation Plan has been approved under clause 12.3(a)(i) or 12.3(a)(ii), the API Council will, as soon as practicable, notify all API Standards Users:
 - (i) that a Minimum Open Banking Implementation Plan has been approved and provide a copy of the approved Minimum Open Banking Implementation Plan; and

- (ii) of the effective date of the Minimum Open Banking Implementation Plan (Implementation Plan Effective Date).
- (b) Implementation Plan Effective Date: The Implementation Plan Effective Date of a Minimum Open Banking Implementation Plan must be no less than 10 Business Days following the date that the API Centre notifies all API Standards Users under sub-clause (a)(i).
- (c) Publication: The API Council must publish a Minimum Open Banking Implementation Plan that has been approved under clause 12.3(a)(i) or 12.3(a)(ii) on the Standards User only section of the API Centre website on or before the Implementation Plan Effective Date.
- (d) Compliance: All API Standards Users must comply with any Minimum Open Banking Implementation Plan on and from the Implementation Plan Effective Date.

12.5 Regular review

The API Council will review the published Minimum Open Banking Implementation Plan on a regular basis, and no less than once annually, to ensure the Minimum Open Banking Implementation Plan continues to meet the recommendation criteria set out in clause 12.2.

13. Breach

13.1 Notification of breach

- (a) Each API Standards User will notify the API Centre as soon as practicable after it becomes aware of a possible breach of any obligation under these Terms which, to avoid doubt, includes:
 - (i) any Unauthorised Use or Customer Data Breach set out in the Data Security Standard by:
 - (A) the API Standards User (the Affected API Standards User); or
 - (B) another API Standards User;
 - (ii) any act or omission of a Permitted User that causes a Third Party to breach clause 7.2.
- (b) An API Standards User who notifies the API Centre of a possible breach under sub-clause (a) must provide the Chief Executive and API Centre Manager with any information requested to enable them to decide:
 - (i) whether the Affected API Standards User has breached these Terms; and
 - (ii) if whether the possible breach, if established, is likely a Trivial Breach, an Intermediate Breach or a Material Breach which includes, without limitation, information about the expected impact of the possible breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;
 - (III) an API Standards User;
 - (IV) a Standardised API; or
 - (B) a Customer or their interests.

13.2 Classification of breach

The Chief Executive, in consultation with the API Centre manager will, upon becoming aware of a possible breach of any obligation under these Terms (either by receipt of a notification made under clause 13.1(a) or by any other means) decide whether the possible breach, if established, is likely to be:

- (a) a Trivial Breach; or
- (b) a breach that is not a Trivial Breach (that is an Intermediate Breach or a Material Breach).

13.3 Trivial Breach procedure

- (a) The Chief Executive will notify the following people as soon as practicable after becoming aware of a possible breach that has been categorised as a Trivial Breach under clause 13.2:
 - (i) the Affected API Standards User; and
 - (ii) if another API Standards User notified the API Centre of the possible Trivial Breach under clause 13.1(a)(i)(B), that API Standards User.
- (b) The notification must:
 - (i) detail the nature of the possible Trivial Breach;
 - (ii) advise that submissions in respect of the possible Trivial Breach can be made to the Chief Executive in writing and specify the date on which submissions must be received; and
 - (iii) advise that submissions should include, to the extent practicable and without limitation, information about the expected impact of the possible breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;
 - (III) an API Standards User;
 - (IV) a Standardised API; or
 - (B) a Customer or their interests.
- (c) The Chief Executive, in consultation with the API Centre Manager, will decide whether the Affected API Standards User has committed a Trivial Breach.
- (d) Before deciding whether an Affected API Standards User has committed a Trivial Breach, the Chief Executive will have regard to:
 - (i) the views of the API Centre Manager;
 - (ii) submissions made within the timeframe prescribed by the Chief Executive under sub-cause (b)(ii) from the following:
 - (A) the Affected API Standards User; and
 - (B) if another API Standards User notified the API Centre of the possible Trivial Breach under clause 13.1(a)(i)(B), that API Standards User.
- (e) Once the Chief Executive has decided whether the Affected API Standards User has committed a Trivial Breach, the Chief Executive will notify the following people as soon as practicable:
 - (i) the Affected API Standards User; and

- (ii) if another API Standards User notified the API Centre of the possible Trivial Breach under clause 13.1(a)(i)(B), that API Standards User.
- (f) If the Chief Executive decides that the API Standards User has committed a Trivial Breach, the Chief Executive will, as soon as practicable:
 - (i) confirm that no further action will be taken;
 - (ii) keep a record the circumstances of the breach and the decision that it was a Trivial Breach; and
 - (iii) notify the Board of Payments NZ of the circumstances of the breach and the decision that it was a Trivial Breach.
- (g) If the Chief Executive decides that the API Standards User has committed a Trivial Breach, the Chief Executive may notify other API Standards Users of the circumstances of the breach and the decision that it was a Trivial Breach.

13.4 Classification of non-Trivial Breach

- (a) If the Chief Executive decides that the possible breach, if established, is likely to be a non-Trivial Breach (that is, an Intermediate Breach or a Material Breach) under clause 13.2(b), the Chief Executive must refer the details of the possible breach to the Independent Committee for consideration.
- (b) The Independent Committee will, upon becoming aware of a possible breach that has been classified as a non-Trivial Breach by the Chief Executive, decide by majority whether the possible breach, if established, is likely to be:
 - (i) an Intermediate Breach; or
 - (ii) a Material Breach.
- (c) The Independent Committee may consult with the Board chair or such other directors that the Board chair may recommend before making a decision that a possible breach, if established, is likely to be a Material Breach.

13.5 Intermediate Breach procedure

- (a) If the Independent Committee decides under clause 13.4 that the possible breach, if established, is likely to be an Intermediate Breach, the Independent Committee will notify the following people as soon as practicable:
 - (i) the Affected API Standards User; and
 - (ii) if another API Standards User notified the API Centre of the possible Intermediate Breach under clause 13.1(a)(i)(B), that API Standards User.
- (b) The notification must:
 - (i) detail the nature of the possible Intermediate Breach;
 - (ii) advise that submissions in respect of the possible Intermediate Breach can be made to the Independent Committee in writing and specify the date on which submissions must be received; and
 - (iii) advise that submissions should include, to the extent practicable and without limitation, information about the expected impact of the possible Intermediate Breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;

- (III) an API Standards User;
 - (IV) a Standardised API; or
 - (B) a Customer or their interests.
- (c) The Independent Committee will decide by majority whether the API Standards User has committed an Intermediate Breach.
- (d) Before deciding whether the API Standards User has committed an Intermediate Breach, the Independent Committee must have regard to the following:
 - (i) submissions made within the timeframe prescribed by the Independent Committee under sub-clause (b)(ii) from the following:
 - (A) the Affected API Standards User;
 - (B) if another API Standards User notified the API Centre of the possible Intermediate Breach under clause 13.1(a)(i)(B), that API Standards User; and
 - (C) any other person that the Independent Committee considers may have a substantial interest in the possible Intermediate Breach;
 - (ii) any other information available that enables the Independent Committee to assess the expected impact of the possible Intermediate Breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;
 - (III) an API Standards User;
 - (IV) a Standardised API; or
 - (B) a Customer or their interests; and
 - (iii) any other information that the Independent Committee considers relevant to the possible Intermediate Breach.
- (e) If the Independent Committee decides that the Affected API Standards User has committed an Intermediate Breach (the Infringing API Standards User), the Independent Committee will, as soon as practicable:
 - (i) do one or more of the following:
 - (A) require the Infringing API Standards User to remedy the Intermediate Breach within a specified period not exceeding three months of the date on which the Infringing API Standards User is notified under sub-clause (ii)(A) below;
 - (B) require the Infringing API Standards User to verify that the Intermediate Breach has been remedied within the timeframe specified;
 - (C) require the Infringing API Standards User to provide evidence of the steps which it has taken to prevent the circumstances giving rise to the Intermediate Breach recurring;
 - (D) make a recommendation to the Board of Payments NZ to require that certain actions are taken by the Infringing API Standards User, including imposing conditions or requirements in relation to the Intermediate Breach;

- (E) if the Infringing API Standards User has not made an Exemption Application, recommend that the Infringing API Standards User make an Exemption Application in accordance with the process set out in clause 15; or
- (F) if the Infringing API Standards User has made an Exemption Application, progress the Infringing API Standards User's Exemption Application in accordance with the process set out in clause 15; and
- (ii) notify the following of its decision (including any actions required by the Independent Committee to remedy the Intermediate Breach under sub-clause (i) above):
 - (A) the Infringing API Standards User;
 - (B) every other API Standards User;
 - (C) the Board of Payments NZ; and
 - (D) the API Centre.
- (f) The Independent Committee will notify the persons specified in sub-clause (e)(ii) if an extension is granted in respect of a timeframe specified in sub-clause (e)(i).
- (g) If the Independent Committee decides that the API Standards User has not committed an Intermediate Breach, the Independent Committee will notify the following people of the decision as soon as practicable after the decision is made:
 - (i) the Affected API Standards User;
 - (ii) if another API Standards User notified the API Centre of the possible Intermediate Breach under clause 13.1(a)(i)(B), that API Standards User; and
 - (iii) if any other person made a submission in accordance with sub-clause (d)(i)(C), that person.

13.6 Material Breach procedure

- (a) The Independent Committee will notify the following people as soon as practicable after deciding that a possible breach, if established, is likely to be a Material Breach under clause 13.4(b)(ii):
 - (i) the Affected API Standards User; and
 - (ii) if another API Standards User notified the API Centre of the possible Material Breach under clause 13.1(a)(i)(B), that API Standards User.
- (b) The notification must:
 - (i) detail the nature of the possible Material Breach;
 - (ii) advise that submissions in respect of the possible Material Breach can be made to the Independent Committee in writing and specify the date on which submissions must be received; and
 - (iii) advise that submissions should include, to the extent practicable and without limitation, information about the expected impact of the possible Material Breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;
 - (III) an API Standards User;

- (IV) a Standardised API; or
 - (B) a Customer or their interests.
- (c) If the Independent Committee decides that a possible breach, if established, is likely to be a Material Breach under clause 13.4(b)(ii), the Independent Committee must refer the details of the Material Breach to the Board of Payments NZ for consideration as soon as practicable.
- (d) The Independent Committee will make a recommendation (Material Breach Recommendation) to the Board of Payments NZ as soon as is practicable on:
 - (i) whether the Independent Committee believes that the Affected API Standards User has committed a Material Breach; and
 - (ii) if so, actions that it recommends that the Affected API Standards User takes to remedy the Material Breach including, without limitation:
 - (A) requiring the Affected API Standards User to remedy the Material Breach within a timeframe specified by the Independent Committee, provide confirmation of such remediation and that the Affected API Standards User has taken all reasonable steps to ensure such Material Breach does not re-occur;
 - (B) requiring the Affected API Standards User to undertake steps specified to remedy the breach within a timeframe specified by the Independent Committee and provide confirmation that the steps have been taken;
 - (C) requiring that certain actions are taken by the Affected API Standards User, including imposing conditions or requirements in relation to the Material Breach. To avoid doubt, in the event of a Material Breach relating to a breach of clause 7.2 by a Third Party due to the acts or omissions of a Permitted User to whom the Third Party has disclosed Customer Data, these actions or requirements may include requiring the Third Party to suspend, terminate or impose conditions on the relevant Permitted User's access to or use of the Standardised API or any Customer Data;
 - (D) if the Affected API Standards User has not made an Exemption Application, recommending that the Infringing API Standards User make an Exemption Application in accordance with the process set out in clause 15;
 - (E) if the API Standards User has made an Exemption Application, recommending that the Exemption Application be approved or declined in accordance with the process set out in clause 15; or
 - (F) suspending the Affected API Standards User.
- (e) The Independent Committee will decide by majority whether to recommend that the API Standards User has committed a Material Breach in the Material Breach Recommendation.
- (f) Before giving the Board of Payments NZ the Material Breach Recommendation, the Independent Committee must have regard to the following:
 - (i) submissions made within the timeframe prescribed by the Independent Committee under sub-clause (b)(ii) from the following:
 - (A) the Affected API Standards;

- (B) if another API Standards User notified the API Centre of the possible Material Breach under clause 13.1(a)(i)(B), that API Standards User; and
 - (C) any other person that the Independent Committee considers may have a substantial interest in the possible Material Breach;
 - (ii) any other information available that enables the Independent Committee to assess the expected impact of the possible Intermediate Breach on:
 - (A) the integrity, security and efficiency of any of the following:
 - (I) the API Centre;
 - (II) the API Centre Register;
 - (III) an API Standards User;
 - (IV) a Standardised API; or
 - (B) a Customer or their interests; and
 - (iii) any other information that the Independent Committee considers relevant to the possible Material Breach.
- (g) Once it has received the Material Breach Recommendation, the Board will, as soon as practicable, decide whether to:
- (i) approve the Material Breach Recommendation;
 - (ii) approve the Material Breach Recommendation subject to any changes the Board of Payments NZ considers appropriate; or
 - (iii) reject the Material Breach Recommendation.
- (h) For the avoidance of doubt, the Board of Payments NZ may decide that the possible breach that is the subject of the Material Breach Recommendation is an Intermediate Breach and decide which actions, if any, set out in the Material Breach Recommendation or in sub-clause (d)(ii) are appropriate in the context of the Intermediate Breach.
- (i) In deciding whether to approve the Material Breach Recommendation, the Board may consider any information that it considers relevant.
- (j) If the Board decides that the API Standards User has committed a Material Breach (the Infringing API Standards User), the Board will notify the following of its decision (including any actions required by the Board to remedy the Material Breach):
- (i) the Infringing API Standards User;
 - (ii) every other API Standards User;
 - (iii) the Independent Committee; and
 - (iv) the API Centre.
- (k) The Board will notify the persons specified in sub-clause (j) if the Board grants an extension in respect of a timeframe given in respect of any action required by the Board to remedy the Material Breach.
- (l) If the Board decides that the API Standards User has not committed a Material Breach, the Board will notify the following of its decision:
- (i) the Affected API Standards User;
 - (ii) if another API Standards User notified the API Centre of the possible Material Breach under clause 13.1(a)(i)(B), that API Standards User;

- (iii) if any other person made a submission in accordance with sub-clause (f)(i)(C), that person; and
- (iv) the Independent Committee.

14. Information gathering and sharing

14.1 API Centre may make enquiries

Each API Standards User consents to the API Centre making such enquiries of, and obtaining such information from, other interested parties (including any relevant regulator) as it considers reasonable with regard to the API Standards User's compliance with these Terms, including with regard to whether or not an API Standards User might have committed, or is likely to commit, a breach of any of these Terms and/or whether or not to make a determination regarding suspension or termination under clause 16 where the API Centre has reason to suspect that the API Standards User may be in Material Breach of these Terms or any Relevant Law.

14.2 Keeping API Centre informed of remedial steps

If an API Standards User is given notice under clauses 13.5(e)(ii) and 13.6(j) to take action in relation to a breach of these Terms, the API Standards User must keep the API Centre up to date and informed of the steps (if any) the API Standards User is taking to address that breach.

14.3 API Standard User notification

The notification and publication obligations set out in clauses 13 and 15 shall not apply in respect of any information regarding an actual or possible breach, or an exemption application (as applicable), if the Independent Director Committee of Payments NZ considers, in its absolute discretion, it is appropriate in the circumstances to withhold that information. In determining whether to withhold any information under this clause 14.3, the Independent Director Committee of Payments NZ may consider:

- (i) whether the information is Confidential Information;
- (ii) whether the publication of the information might cause unreasonable harm to any party;
- (iii) whether notification or publication would undermine the integrity, security and efficiency of the API Centre or a Standardised API;
- (iv) the views of the applicant API Standards User; and
- (v) any other matters the Independent Director Committee of Payments NZ considers to be relevant.

15. Exemptions

15.1 Exemption from obligations

- (a) Where an API Standards User (**the Applicant**) wishes to be exempt from one or more obligations under these Terms, it may submit a written application for an exemption to the API Centre Manager. Such application must include the following information:
 - (i) the obligation, or obligations, in respect of which the exemption is being sought (including, without limit, details of any provisions in these Terms, or requirements or functionality in an Operational Standard or an API Standard from which an exemption is sought);

- (ii) the rationale as to why the exemption is being sought;
- (iii) whether the application is for a permanent or temporary exemption and, if the application is for a temporary exemption, how long the exemption is required for;
- (iv) if relevant, a detailed plan for how and when the Applicant will be compliant with the obligation in respect of which the exemption is being sought;
- (v) whether the Applicant considers that granting or not granting the exemption would undermine the purpose of the API Centre to promote system efficiency, security, safety and customer uptake through the use of interoperable API Standards by API Standards Users or have a material adverse impact on:
 - (A) the integrity, security and efficiency of the API Centre;
 - (B) any API Standards User;
 - (C) the integrity, security and efficiency of a Standardised API; and/or
 - (D) a Customer's interests;
 - (E) any other requirements the Chief Executive or Independent Committee (as applicable) may deem necessary from time to time,
 (an Exemption Application).
- (b) To avoid doubt, Exemption Applications may be submitted by an API Standards User at any time, including upon that API Standards User becoming aware, or being notified, that it has committed, or has possibly committed, a breach of these Terms or during a breach determination procedure set out in clause 13.

15.2 Notification and submissions

- (a) Subject to sub-clause (c), within five Business Days of receipt of the Exemption Application, the API Centre will notify all API Standards Users of the Exemption Application and the name of the Applicant for the purposes of allowing API Standards Users the opportunity to make a submission in respect of any such application.
- (b) Where an API Standards User wishes to make a submission regarding an Exemption Application, such submissions must be made within 10 Business Days of the notification made by the API Centre under sub-clause (a), or such later date as may be determined by the API Centre Manager.
- (c) To avoid doubt, the API Centre is not required to notify API Standards Users where the Exemption Application is determined by the API Centre to be in respect of a Trivial Breach.

15.3 Exemption Application review procedure

- (a) Referral to the Chief Executive: The API Centre Manager will refer the following Exemption Applications to the Chief Executive for determination:
 - (i) where the Exemption Application seeks an exemption for a timeframe of less than three months; or
 - (ii) where the Exemption Application relates to compliance with a minor technical specification in a Standardised API (whether or not the Exemption Application seeks an exemption for a timeframe of less than three months).
- (b) Referral to Independent Committee: The API Centre Manager will refer all other Exemption Applications to the Independent Committee for determination.

- (c) Chief Executive and Independent Committee decision: Once an Exemption Application has been referred to the Chief Executive or Independent Committee for determination, the Chief Executive or Independent Committee (as applicable) will, as soon as is practicable, make a determination to:
 - (i) approve the Exemption Application;
 - (ii) approve the Exemption Application subject to any conditions the Chief Executive or Independent Committee (as applicable) considers appropriate or;
 - (iii) reject the Exemption Application.
- (d) Required considerations: When assessing an Exemption Application, the Chief Executive or Independent Committee (as applicable) must consider:
 - (i) any submissions made by the Applicant;
 - (ii) any submissions made by any other API Standards Users; and
 - (iii) the results of any related Independent Assessment obtained under sub-clause (e).
- (e) Independent Assessment:
 - (i) In making a determination in relation to an Exemption Application, the Chief Executive or Independent Committee (as applicable) may, subject to sub-clause (iii) below, engage an independent and relevantly qualified specialist to perform an independent technical assessment of the Exemption Application (Independent Assessment).
 - (ii) The Applicant must bear the cost of obtaining the Independent Assessment.
 - (iii) The Chief Executive or Independent Committee (as applicable) must notify the Applicant of the intention to commission an Independent Assessment and inform the Applicant of the estimated costs involved in obtaining that assessment and that it must bear the costs of that assessment.
- (f) Withdrawing an Exemption Application: The applicant may withdraw an Exemption Application at any time before a decision is made by the Chief Executive or Independent Committee (as applicable).

15.4 Notification of determination

- (a) Subject to clause 14.3, the API Centre will, as soon as practicable, notify the following after a determination is made by the Chief Executive or Independent Committee in relation to an Exemption Application:
 - (i) the Applicant; and
 - (ii) every other API Standards User.
- (b) If a determination is made to approve an Exemption Application in relation to compliance with an Implementation Plan, the API Centre will, subject to clause 14.3, publish the details of the Applicant and the exemption, including any conditions, on the public API Centre website.

15.5 Approval of Exemption Application

- (a) Grounds for approval: An Exemption Application may only be approved if the Chief Executive or Independent Committee (as applicable) is satisfied that granting the exemption will not undermine the purpose of the API Centre to promote system efficiency, security, safety and customer uptake through the use of interoperable API Standards by API Standards Users.

- (b) Considerations in making determination: When making a determination in relation to an Exemption Application, the Chief Executive or Independent Committee (as applicable) must consider the extent to which granting, or not granting, the Exemption Application would have a material adverse impact on:
 - (i) the integrity, security, and efficiency of the API Centre;
 - (ii) any API Standards User;
 - (iii) the integrity, security, and efficiency of a Standardised API; and
 - (iv) a Customer's interests.
- (c) Conditions of approval: When approving an Exemption Application, the Chief Executive or Independent Committee (as applicable) must set the duration of the exemption, and may impose such conditions on the Applicant as the Chief Executive or Independent Committee (as applicable) considers reasonable, including:
 - (i) reporting requirements;
 - (ii) undertakings;
 - (iii) indemnity obligations on the Applicant; and/or
 - (iv) any other conditions the Chief Executive or Independent Committee (as applicable) deems necessary.

15.6 Extension and appeal procedures

- (a) Extensions: An Applicant who has been granted an exemption may, at any time up until three weeks prior to the expiry of the exemption, apply for an extension of the exemption. An application to extend an exemption will be referred to the Chief Executive or Independent Committee (depending on who approved the Exemption Application) and will be determined in accordance with the processes and requirements set out in this clause 15.
- (b) Notification: Subject to clause 18.3, the API Centre will, as soon as practicable, notify the following after the Chief Executive or Independent Committee (as applicable) makes a determination in relation to an application for an extension under sub-clause (a):
 - (i) the Applicant; and
 - (ii) every other API Standards User.
- (c) If a determination is made to extend an exemption in relation to compliance with an Implementation Plan, the API Centre will, subject to clause 18.3, publish the details of the extended exemption, including any conditions, on the public API Centre website.
- (d) Appeals: Subject to clause 14.3:
 - (i) If an Applicant is dissatisfied with any determination made by the Chief Executive in response to an Exemption Application (or an application for an extension to an existing exemption under subclause (a)), including any conditions imposed by the Chief Executive when approving an Exemption Application, the Applicant may appeal the decision of the Chief Executive to the Independent Committee.
 - (ii) If an Applicant is dissatisfied with any determination made by the Independent Committee in response to an Exemption Application (or an application for an extension to an existing exemption under subclause(a)), including any conditions imposed by the Independent Committee when approving an Exemption Application, the Applicant may appeal the decision of

the Independent Committee to the Independent Director Committee of Payments NZ.

- (e) Notification of Appeal: The API Centre will, as soon as practicable after receipt of notification of an appeal, notify all API Standards Users and the original decision maker.
- (f) Appeal procedure and requirements: Subject to clause 18.3:
 - (i) An appeal request made by an Applicant (**the Appeal**) must be made in writing no later than 10 Business Days after the date of receiving notice of the decision which is being appealed, or such later date as may be agreed by the Chief Executive.
 - (ii) In considering the Appeal, the Independent Committee or Independent Director Committee of Payments NZ (as applicable) can request written submissions from the Applicant and/or the original decision-maker and take into account any information that it considers relevant to the Appeal.
 - (iii) The Independent Committee or the Independent Director Committee of Payments NZ may confirm, reverse or vary the decision that is the subject of the Appeal. The Independent Committee or Independent Director Committee of Payments NZ may, if it considers appropriate, refer the Appeal back to the original decision maker for reconsideration of the Exemption Application.
 - (iv) Where the Independent Committee or Independent Director Committee of Payments NZ reverses or varies a determination made by the Chief Executive or Independent Committee, it may only do so if it determines that the initial determination that is the subject of the Appeal (or part thereof) made by the Chief Executive or Independent Committee was not one of a range of decisions that could reasonably be made.
- (g) Notification of determination
 - (i) The API Centre will, as soon as practicable, notify the following of a determination made by the Independent Committee or Independent Director Committee of Payments NZ in relation to the Appeal:
 - (A) the original decision maker;
 - (B) the Applicant; and
 - (C) every other API standards User.
 - (ii) The API Centre will, as soon as practicable, notify the following if the Independent Committee or Independent Director Committee of Payments NZ refers the Appeal back to the original decision maker for reconsideration of the Exemption Application:
 - (A) the Applicant; and
 - (B) every other API Standards User.

16. Suspension and termination of API Standards User

16.1 Grounds for suspension of an API Standards User

An API Standards User's Registration may be suspended if the API Standards User:

- (a) has been found to be in Material Breach of these Terms in accordance with clause 13.6; or

- (b) is subject to an Insolvency Event,
(each of the above, a Ground for Suspension).

16.2 Consequences of suspension

Upon suspension of an API Standards User's Registration:

- (a) the API Standards User's right to use the API Standards or a Standardised API with another API Standards User any Permitted Users, any Outsourced Providers and/or any PoC Partners is suspended;
- (b) the API Centre will notify all API Standards Users of the suspension of that API Standards User's Registration as soon as practicable following such suspension and may take such other steps as are reasonable and practicable in the circumstances to mitigate any damage arising or that may arise from such suspension;
- (c) the parties to any Bilateral Agreement to which the suspended API Standards User is a party must, without delay, consider the Customer Related Service repercussions of the suspension as well as the Grounds for Suspension, and take immediate steps to protect the integrity, security and efficiency of the API Centre or a Standardised API or Customers, and, if required by the API Centre, suspend, with immediate effect, the relevant parts of the Bilateral Agreement, being the parts that relate to the use of the API Standards or a Standardised API;
- (d) the API Standards User must notify its Customers that have any current Customer Consents with the API Standards User of the suspension, that the Customer Consents may be revoked and the effect of any revocation;
- (e) the API Centre will update the Register User Account by recording the status of the API Standards User as "revoked" and remove that API Standards User's access to its Register User Account; and
- (f) the API Centre will update the register of API Standards Users on its website by recording the suspension of the API Standards User.

16.3 Application for reinstatement of Registration

An API Standards User who has had its Registration suspended may at any time apply to the API Centre for revocation of suspension of its Registration, if the API Standards User provides the API Centre with:

- (a) evidence that it meets the Registration Criteria and that it has remedied the matters that gave rise to the suspension;
- (b) evidence of the steps that it has taken to prevent the matters that gave rise to the suspension recurring; and
- (c) any additional information reasonably required by the API Centre.

16.4 Consideration of reinstatement by API Centre

- (a) The API Council must:
 - (i) consider any application by an API Standards User for revocation of suspension of Registration; and
 - (ii) subject to the approval of the Board of Payments NZ, either revoke or confirm the suspension.
- (b) As soon as practicable after the API Council makes a determination in respect of an application under paragraph (a) above, the API Centre must notify every API Standards User of the determination by publishing details on its website.

- (c) If the API Council, revokes the suspension, it must determine the date on which the revocation takes effect and advise the API Standards User of that date.
- (d) If the API Council confirms the suspension, it must notify the API Standards User that its Registration may be terminated in accordance with these Terms.

16.5 Termination of an API Standards User's Registration

- (a) The API Council may, with the approval of the Board of Payments NZ, terminate an API Standards User's Registration as an API Standards User if:
 - (i) the API Standards User has had its Registration suspended and has not, within 6 months after the date that the API Standards User was notified that its Registration as an API Standards User was suspended, applied for that suspension to be revoked under clause 16.3; or
 - (ii) the API Standards User has applied to the API Council for revocation of suspension of Registration and the API Council has determined not to revoke the suspension of the API Standards User's Registration in accordance with clause 16.4; or
 - (iii) the API Council, determines, in its sole discretion, that the provision of the API Standards to the API Standards User is prohibited by any Relevant Law or has become impractical or unfeasible for any legal, regulatory, or other reason; or
 - (iv) the API Standards User has been unable to perform its obligations under the Terms due to a Force Majeure Event and that failure has not been mitigated or remedied within 90 days of the Force Majeure Event first occurring.
- (b) If the API Council decides to terminate an API Standards User's Registration, it must:
 - (i) determine a time and date on which the termination will take effect; and
 - (ii) give written notice of the termination and the time and date on which the termination will take effect to all API Standards Users, including the affected API Standards User.

16.6 Consequences of termination

On and from the time and date that an API Standards User's Registration has been terminated in accordance with clause 16.5:

- (a) the terminated API Standards User's right to use the API Standards or a Standardised API with another API Standards User, any Permitted Users, any Outsourced Providers and/or any PoC Partners is revoked;
- (b) subject to subclause (c) of this clause 16.6, the terminated API Standards User must stop using the API Standards and any Standardised API with another API Standards User, any Permitted Users, any Outsourced Providers and/or any PoC Partners;
- (c) the relevant parts of a Bilateral Agreement which the terminated API Standards User has entered into with a Bilateral Counterparty, being the parts that relate to the use of the API Standards or a Standardised API must be terminated with immediate effect, except where the Customer Related Service repercussions of such immediate termination are not able to be appropriately managed in the Customer's interests. If this is the case, the terminated API Standards User and its Bilateral Counterparty must take immediate steps to agree a future date (no later than 30 days following the date on which the API Centre notified all API Standards Users of the termination of the terminated API Standards User's Registration) by which:
 - (i) the relevant parts of the Bilateral Agreement are to be terminated; and

- (ii) all or some of the Customer Related Services provided under the Bilateral Agreement are suspended until the parties can enter into a new or amended agreement outside the scope of the API Centre;
- (d) the API Standards User must notify its Customers that have any current Customer Consents with the API Standards User of the termination and, if the Customer requests it to do so, delete, destroy or anonymise all Customer Data that the API Standards User holds that was acquired through, or created as an outcome of, using a Standardised API in accordance with a Customer Consent (and must ensure that any Outsourced Provider or Permitted User that is in custody of such Customer Data also destroys, deletes, or anonymises such Customer Data (unless and to the extent that Customer has expressly consented to such parties retaining such data following the revocation of the Customer Consent)), except to the extent that any Customer Data must be retained by a law or relates to any current or anticipated legal proceedings or dispute resolution proceedings;
- (e) the terminated API Standards User must, as soon as practicable, remove any express or implied connection to the API Centre, the API Standards or to Standardised APIs;
- (f) the API Centre must, as soon as practicable, update the Register User Account recording the API Standards User's status as "revoked" and remove that API Standards User's access to its Register User Account;
- (g) the API Centre must, as soon as practicable, update the register of API Standards Users on its website by removing that terminated API Standards User from the register;
- (h) the API Centre may, at its option, publish a notice on its website stating that the terminated API Standards User has ceased, or will cease, to be an API Standards User; and
- (i) the API Centre may take such other steps as are reasonable and practicable in the circumstances to mitigate any damage arising or that may arise from such termination, including any impact on Customer Related Services.

17. Effect of suspension or termination

17.1 Survival

Suspension or termination by the API Centre of an API Standards User's Registration does not affect any right or obligation that arose under these Terms before such suspension or termination, and is without prejudice to either party's other rights and remedies in respect of those rights and obligations. While termination of an API Standards User's Registration terminates the parties' contractual relationship under these Terms, termination does not affect any provision of these Terms which is expressly or by implication intended to come into force on or after termination, or which is expressly or by implication intended to continue in force after such termination.

17.2 Specific effects

Without limiting any other provision of these Terms, upon suspension or termination of an API Standards User's Registration for any reason:

- (a) each party will act in the spirit of co-operation in order to have as minimal an impact upon other API Standards Users and Customers as is reasonably possible having regard to the obligations in these Terms;

- (b) that API Standards User is responsible for notifying its Bilateral Counterparties, and its Customers (as required), of the suspension or termination and for any support required to be provided to such persons following such suspension or termination;
- (c) all licences for branding granted to the API Centre by the API Standards User under these Terms will be suspended (in the case of suspension) or terminated (in the case of termination) immediately;
- (d) all rights and authorisations granted to the API Standards User under these Terms will be suspended (in the case of suspension) or terminated (in the case of termination) immediately, subject to the limited authorisation to continue to operate under amended Bilateral Agreements for a limited period with other API Standards Users where the interests of Customers would otherwise be compromised, and:
 - (i) the relevant API Standards User must:
 - (A) promptly cease using all branding or other references to the API Standards, Standardised APIs or the API Centre;
 - (B) no longer represent to any person that the API Standards User is using the API Standards or Standardised APIs;
 - (C) if requested by the API Centre, and as soon as practicable, return to or destroy all Confidential Information of the API Centre in its possession or control, except to the extent that it is required by Relevant Law to retain the Confidential Information; and
 - (D) if requested by the API Centre, provide a certificate to the API Centre stating that, to the best of its knowledge and belief, the Confidential Information returned or destroyed comprises all the Confidential Information in its possession or control (other than in respect of the permitted exceptions in paragraph 17.2(d)(i)(C));
 - (ii) the API Centre must:
 - (A) if requested to do so by the API Standards User, return to or destroy all Confidential Information of the API Standards User in its possession or control, except to the extent it is required by Relevant Law to retain Confidential Information or it reasonably requires the Confidential Information to undertake its obligations under these Terms; and
 - (B) if requested to do so by the API Standards User, provide a certificate to the API Standards User stating that, to the best of its knowledge and belief, the Confidential Information returned or destroyed comprises all the Confidential Information in its possession or control (other than in respect of the permitted exceptions in paragraph 17.2(d)(ii)(A)).

18. Withdrawal from being an API Standards User

18.1 Withdrawal

- (a) An API Standards User may, at any time, withdraw from being an API Standards User by giving not less than 30 Business Days' written notice to the API Centre.
- (b) Notwithstanding sub-clause (a) and subject to sub-clause (c), an API Standards User may withdraw from being an API Standards User with immediate effect by giving written notice to the API Centre if the API Standards User receives an invoice from the API Centre which provides that the applicable Annual API Standards User Fee has increased.

- (c) An API Standards User that withdraws in accordance with sub-clause (b) must withdraw no later than 30 days after receiving the updated invoice.
- (d) The API Standards User is responsible for notifying its Bilateral Counterparties of the withdrawal.
- (e) All licences for branding granted to and by the API Centre and the API Standards User under these Terms will be terminated from the effective date of withdrawal.
- (f) All rights and authorisations granted under these Terms will be terminated from the effective date of withdrawal, and:
 - (i) the API Standards User must:
 - (A) promptly cease using all branding or other references to the API Standards, Standardised APIs or the API Centre;
 - (B) return to or destroy all Confidential Information of the API Centre in its possession or control, except to the extent that it is required by Relevant Law to retain the Confidential Information; and
 - (C) if requested by the API Centre, provide a certificate to the API Centre stating that, to the best of its knowledge and belief, the Confidential Information returned or destroyed comprises all the Confidential Information in its possession or control (other than in respect of the permitted exceptions in paragraph 18.1(f)(i)(B));
 - (ii) the API Centre must:
 - (A) if requested to do so by the API Standards User, return or destroy all Confidential Information of the API Standards User in its possession or control, except to the extent that it is required by Relevant Law to retain Confidential Information or it reasonably requires the Confidential Information to undertake its obligations under these Terms; and
 - (B) if requested to do so by the API Standards User, provide a certificate to the API Standards User stating that, to the best of its knowledge and belief, the Confidential Information returned or destroyed comprises all the Confidential Information in its possession or control (other than in respect of the permitted exceptions in paragraph 18.1(f)(ii)(A)).

18.2 Consequences of withdrawal

If an API Standards User withdraws from being an API Standards User:

- (a) on and from the date on which the withdrawal takes effect (which should take into account the need to manage the interests of Customers accessing Customer Related Services provided under Bilateral Agreements), the API Standards User's Registration and authorisation to use the API Standards will be revoked, and the API Standards User must stop using the API Standards and any Standardised API with another API Standards User, any Permitted Users, any Outsourced Providers and/or any PoC Partners;
- (b) the API Standards User must notify its Customers that have any current Customer Consents with the API Standards User of the withdrawal and, if the Customer requests it to do so, delete, destroy or anonymise all Customer Data that the API Standards User holds that was acquired through, or created as an outcome of, using a Standardised API in accordance with a Customer Consent (and must ensure that any Outsourced Provider, Technical Service Provider or Permitted User that is in custody of such Customer Data also destroys, deletes, or anonymises such Customer

Data (unless and to the extent that Customer has expressly consented to such party retaining such data following the revocation of the Customer Consent)), except to the extent that any Customer Data must be retained by a law or relates to any current or anticipated legal proceedings or dispute resolution proceedings;

- (c) the API Centre will update the Register User Account by recording the status of the API Standards User as “revoked” and remove that API Standards User’s access to its Register User Account;
- (d) the API Centre will update the register of API Standards Users on its website and remove the API Standards User from the register; and
- (e) the API Centre may also, at its option, publish a notice on its website stating that the relevant API Standards User has ceased, or will cease, to be an API Standards User.

19. Suspension or termination of the use of particular API Standards

- (a) The API Centre, with the approval of the Board of Payments NZ, may suspend or terminate the use of any one or more API Standards or Operational Standards, in its sole discretion, in whole or in part:
 - (i) immediately (while giving as much notice as is reasonably practicable), if the API Centre is required to do so by law; or
 - (ii) immediately (while giving as much notice as is reasonably practicable), to protect the integrity, security and efficiency of the API Centre or the integrity, security and efficiency of a Standardised API or any Customer Data, or to respond to any systemic risk; or
 - (iii) on 180 days’ written notice to each API Standards User, for any reason.
- (b) Clause 17 of these Terms will apply upon suspension or termination of the use of any one or more API Standards in accordance with this clause 19, but only in relation to the particular API Standard or Operational Standard that has been suspended or terminated.

20. Complaints and Disputes

20.1 Complaints and Disputes between the API Centre and an API Standards User

Complaints and disputes between the API Centre and an API Standards User will be resolved as follows:

- (a) each party must, to the extent possible, continue to perform its obligations under these Terms even if there is a dispute;
- (b) either party may give the other party (the second party) notice of the nature and details of the dispute, and the parties will use best efforts to resolve that dispute through good faith negotiations directly with the other party;
- (c) if the dispute is not resolved within 20 Business Days’ of receipt of the notice of dispute by the second party, either party may by notice to the other party refer the dispute to mediation, and the following shall apply:
 - (i) the mediation will be conducted in Wellington by a mediator who is a member of the Arbitrators’ and Mediators’ Institute of New Zealand (AMINZ); and

- (ii) if the parties do not agree on a mediator within five Business Days' of receipt of the notice of mediation, the mediator will be appointed or the fees set by the President of AMINZ (or his/her nominee) at the request of either party;
- (d) the parties will bear the mediator's fees equally; and
- (e) no party may commence any proceedings relating to any dispute between the parties unless the party has taken all reasonable steps to comply with this clause. However, nothing in this clause 20 will preclude a party from seeking urgent interlocutory relief before a court.

20.2 Complaints and Disputes between Bilateral Counterparties

If there is a dispute between Bilateral Counterparties, then the parties will follow the process set out for the resolution of disputes in the relevant Bilateral Agreement (if any), provided that the parties may at any time agree to refer the dispute to the Independent Committee for consideration against the principles of participation and objectives of the API Centre. The Independent Committee may provide guidance or recommendations to the parties to assist them to resolve the dispute.

21. Liability

21.1 Waiver of Liability of the API Centre to API Standards User

- (a) The API Centre is not responsible or liable for any API Standards User's failure to comply with these Terms or for the performance of any obligation or exercise of any right (or failure to perform any obligations or exercise any right) by an API Standards User, Permitted User, Outsourced Provider, PoC Partner or Customer.
- (b) To the maximum extent permitted by law, the API Centre is not liable for, and each API Standards User releases and waives all claims against the API Centre and its officers, employees and agents from, any and all loss, claims, damages, costs and expenses (including litigation costs and legal fees) or other liability of any kind, including:
 - (i) arising from or in any way related to an API Standards User's use of the API Standards, Operational Standards, the API Centre, the API Centre Register or any Customer Data;
 - (ii) arising from or in any way related to the performance of any obligations or exercise of any rights or powers under these Terms by the API Centre, the Board of Payments NZ or the Independent Committee; or
 - (iii) incurred by either an applicant (at the time of applying) or an API Standards User arising out of or in connection with the API Centre.
- (c) The limitation of liability under paragraph (b) above will not apply to the API Centre's liability for losses incurred by an API Standards User due to gross negligence, fraud or wilful misconduct of the API Centre or its officers, employees or agents, or breach of the API Centre's obligations in clause 23(c) or clause 26.
- (d) To the maximum extent permitted by law, the API Centre will not in any event be liable to any API Standards User for any:
 - (i) incidental, indirect or consequential loss of any kind;
 - (ii) loss of profits or revenue; or
 - (iii) loss of, or corruption to, data.

21.2 No Warranties

The API Centre:

- (a) does not make any warranty or representation regarding the API Standards, the API Centre Register or Industry Sandbox, including warranties as to description, merchantability, that the API Standards, the API Centre Register or Industry Sandbox will be free from defects, Viruses or are otherwise fit for the purposes required by the API Standards Users, Customers, Outsourced Providers, PoC Partners or Permitted Users; and
- (b) to the extent permitted by law, excludes all warranties and guarantees that may be implied by law.

21.3 Further limitation of liability of the API Centre

To the extent that the liability of the API Centre cannot be excluded by law, or is not excluded by these Terms, the maximum total liability of the API Centre to any API Standards User, whether that liability arises under contract, tort (including negligence), by statute or otherwise, is limited to losses or damages up to an amount not exceeding the aggregate amount of fees paid to the API Centre by the API Standards User in the 12 months immediately preceding the most recent event giving rise to liability.

21.4 Application of this clause to API Centre related persons and groups

The limitations and exclusions of liability in this clause 21 also apply to the members of the API Council, members of the API Independent Committee, Payments NZ, the Board and Chief Executive of Payments NZ and the officers, employees and agents of Payments NZ or the API Centre, such that any reference to "API Centre" in this clause 21 is also deemed to be a reference to such persons or groups. This clause 21 is for the benefit, and enforceable at the suit, of such persons or groups.

21.5 Liability between API Standards Users

Liability as between an API Provider and a Third Party will be agreed between the parties in any Bilateral Agreement entered into, provided that the following principles must be followed:

- (a) each party is liable for the acts and omissions of its officers, employees and agents which:
 - (i) in the case of Third Parties, may include Technical Service Providers, Outsourced Providers and Permitted Users); and
 - (ii) in the case of API Providers, may include Outsourced Providers and PoC Partners; and
- (b) to the extent possible, the liability framework agreed between the parties must be consistent with existing legal frameworks and market practices to ensure that there is no uncertainty about liability and the rights of Customers.

21.6 Cap on Liability

Except in the case of gross negligence, fraud or wilful misconduct, the liability of a Third Party under these Terms, including in respect of its liability under the indemnity contained in clause 22, shall be limited to the amount prescribed by the API Centre from time to time and set out in Appendix 2.

21.7 Evidence of Insurance

Each Third Party must at all times hold insurance cover for the amount of the liability cap prescribed by the API Centre from time to time and provide the API Centre:

- (a) with evidence that it holds such insurance cover for the amount of the liability cap applying to it at the time that it accedes to these terms and conditions; and
- (b) if reasonably requested by the API Centre, with evidence that it continues to hold such insurance cover for the amount of the liability cap prescribed by the API Centre from time to time.

22. Indemnity of the API Centre

22.1 Indemnity against External Third Party Claims

- (a) Each API Standards User assumes all risks and liability inherent in its use of the API Standards, Operational Standards and API Centre Register and indemnifies and holds harmless Payments NZ, the API Centre, the API Council, API Independent Committee, the Board and Chief Executive of Payments NZ and the officers, employees and agents of Payments NZ or the API Centre (each an "Indemnified Party") from and against all claims, liabilities, damages, losses and expenses (including legal expenses on a solicitor-client basis) suffered or incurred by an Indemnified Party in relation to any External Third Party Claim resulting from that API Standards User's:
 - (i) breach of these Terms;
 - (ii) failure to implement reasonable security safeguards, which contributes to an information technology system breach affecting any Standardised API, Customer, or Customer Data;
 - (iii) failure to comply with Relevant Laws;
 - (iv) acts or omissions giving rise to payment risk (that is where a Customer payment has been initiated or approved by an API Provider but is subsequently cancelled or dishonoured due to an act or omission of the API Standards User in breach of these Terms or a Bilateral Agreement);
 - (v) infringement of a third party's proprietary or Intellectual Property Rights;
 - (vi) failure to fulfil its obligations to a Customer under any contract for services utilising the API Standards, Standardised APIs and the API Centre Register;
 - (vii) use of trade marks relating to the API Standards, Operational Standards or API Centre, other than in accordance with these Terms;
 - (viii) breach of any Customer contract (i.e., a failure to fulfil a contract with a Customer) or breach of any Customer Consent;
 - (ix) breach of confidentiality obligations; or
 - (x) gross negligence, fraud or wilful misconduct.
- (b) For the purposes of this clause 22.1, "External Third Party Claim" means any claim, action, proceeding (including arbitration) demand or allegation that a person who is not a party to the relevant API Centre Agreement makes, asserts, commences or threatens against any Indemnified Party.

22.2 Indemnity from API Providers

Each API Provider indemnifies and holds harmless each Indemnified Party against all claims, liability, damages, losses, and expenses (including legal expenses on a solicitor-client basis) ("loss"), suffered or incurred by the Indemnified Party in connection with an API Centre Agreement as a result of the actions or inactions of a Third Party, which that Indemnified Party has sought to recover directly from that Third Party under an API Centre Agreement

but has not been able to recover from the Third Party due to the liability cap in clause 21.6 being exceeded. The indemnity in this clause is provided on the following basis:

- (a) where the Third Party has entered into a Bilateral Agreement with only one API Provider, that API Provider will indemnify the Indemnified Parties;
- (b) where the Third Party has entered into Bilateral Agreements with more than one API Provider,
 - (i) and the loss can be directly related to the Third Party's actions or inactions with an API Provider, that API Provider will indemnify the Indemnified Parties for that loss; and
 - (ii) in all other circumstances, each of the API Providers with whom the Third Party has a Bilateral Agreement jointly and severally indemnify the Indemnified Parties.

22.3 Exceptions

An API Standards User will not be liable under the indemnity in clause 22.1 or 21.2 to the extent that any Indemnified Party causes, or does not take reasonable steps to mitigate, the relevant loss.

22.4 Control of claims

Where an External Third Party Claim arises:

- (a) the API Standards User will have the option of controlling the conduct or defence of any External Third Party Claim and all negotiations for its settlement or compromise, and may elect to exercise that option by written notice to the Indemnified Party. Where the API Standards User elects to control the conduct or defence of the claim and negotiations, the API Standards User:
 - (i) will consult with the Indemnified Party and keep them fully informed of the progress of the External Third Party Claim; and
 - (ii) ensure that the Indemnified Party's name and business reputation are not materially adversely affected by any such steps taken; and
- (b) at the API Standards User's request and cost, the Indemnified Party will provide all reasonable assistance and co-operation to the API Standards User in relation to defending or settling any External Third Party Claim and will make its employees available to give statements, information and evidence as the API Standards User may reasonably request.

23. Key Contacts

- (a) Each API Standards User will provide the API Centre with the following information in relation to each of its Key Contacts:
 - (i) Name;
 - (ii) Email address; and
 - (iii) Phone number.
- (b) Each API Standards User confirms and warrants on an ongoing basis that it has obtained consents from its Key Contacts for their name, email, and phone number to be made available to all other API Standards Users via the register of Key Contacts. Each API Standards User and the API Centre acknowledge that the register of Key Contacts constitutes and includes Confidential Information.

- (c) The API Centre will hold and manage personal information of Key Contacts in accordance with Relevant Law.

24. Ownership of Licensing and Intellectual Property Rights

24.1 Intellectual Property Rights

Nothing in these Terms transfers ownership of any:

- (a) Intellectual Property Rights of the API Centre or an API Standards User that existed prior to the date of Registration of the API Standards User, or that have been developed independently by either party; or
- (b) modification, translation, adaption, or development of such Intellectual Property Rights, unless otherwise agreed.

Without limiting this clause 24.1, an API Standards User will not acquire any right, title, or interest in any Intellectual Property Rights in the API Centre, the API Standards or the Operational Standards by reason of being an API Standards User.

24.2 Licence of Brands

- (a) The API Centre grants each API Standards User a non-exclusive, non-transferable, non-sub-licensable licence to reproduce the API Centre brand (as advised by the API Centre from time to time), use the API Centre compliance marks (if any), and to publicise its participation in the API Centre, for the purpose of that API Standards User's use of the API Standards. The API Standards User will follow the relevant brand guidelines advised by the API Centre from time to time.
- (b) Each API Standards User grants the API Centre a royalty free licence to reproduce the API Standards User's brand (as advised by the API Standards User from time to time) on the Standards User only section of the API Centre website and any publications to publicise the API Standards User's use of the API Standards. When using the API Standards User's brand, the API Centre will follow the relevant brand guidelines advised by the API Standards User from time to time.
- (c) Neither party will modify the other party's brand.
- (d) Each API Standards User's rights and licence to use the API Centre brand will immediately be suspended or revoked in accordance with clause 20 or 21 of these Terms, if the API Standards User's Registration is suspended, terminated, or revoked.
- (e) The API Centre's rights and licence to use an API Standards User's brand will immediately be revoked if that API Standards User's Registration is terminated or revoked and the API Centre must cease using that API Standards User's brand without unreasonable delay.

25. Governance

- (a) Payments NZ has established:
 - (i) the API Centre to develop, maintain and publish API Standards and govern the use of API Standards by API Standards Users;
 - (ii) the API Council to assist in the performance of the functions of the API Centre; and

- (iii) an Independent Committee of the API Council which will consider, advise and provide recommendations on matters relevant to the API Centre, particularly where conflicts of interest arise.
- (b) The API Council will be appointed by the Board of Payments NZ, and will undertake its responsibilities, in accordance with the API Council Charter published by Payments NZ from time to time.

26. Confidentiality

Each recipient of Confidential Information of another party must:

- (a) ensure such Confidential Information is treated as confidential;
- (b) use such Confidential Information only for the purposes of exercising its rights or fulfilling its obligations under these Terms;
- (c) ensure such Confidential Information is not disclosed to any other person except:
 - (i) as expressly permitted in these Terms; or
 - (ii) to such of its employees and employees of its Related Entities who reasonably require that information in order to perform their roles, and who have agreed to obligations of confidentiality and use that are no less protective than this clause 26; or
 - (iii) with the consent of the provider of the Confidential Information; or
 - (iv) as required by Relevant Law (including under the Privacy Act 2020); or
 - (v) in the case of a party which is a listed issuer, as required by any recognised exchange on which the securities of that party are listed; or
 - (vi) if the information is generally publicly available; or
 - (vii) to its legal advisers and auditors for the purpose of considering or advising on the Confidential Information; or
 - (viii) as reasonably necessary to give effect to, or enforce, these Terms;
- (d) where disclosure is required by law or a securities exchange, the recipient must:
 - (i) promptly and to the extent permitted by Relevant Law, notify the other party of the requirement to disclose, the information it will disclose, the date of disclosure, and the action it proposes to take;
 - (ii) allow the other party an opportunity to oppose such a requirement (if possible);
 - (iii) only disclose that portion of Confidential Information which the party is required to disclose by Relevant Laws, a regulator, a court of competent jurisdiction, or the rules of the relevant securities exchange; and
 - (iv) take all the steps permitted in such judicial, regulatory or administrative process to preserve the confidentiality of the Confidential Information.

27. Notices

27.1 API Standards Users to notify any change of address

API Standards Users must provide written notice to the API Centre of any changes in their address for notices and contact details for the purposes of these Terms, including any changes to Key Contacts.

27.2 Address for Notices

Except to the extent that a party has notified the other party that it has particular notice requirements for delivery of notices and the other party has agreed to such requirements, a notice required by these Terms to be sent to a party may be:

- (a) sent electronically to the last address provided by that party to the other party for the receipt of documents electronically, including sending by email or by an application; or
- (b) delivered to that party; or
- (c) posted to that party's address (which in the case of an API Standards User, will be the address shown in the register of API Standards Users, or such other address as may have been notified in writing to the API Centre by the API Standards User).

27.3 Timing of receipt

A notice is deemed to be received:

- (a) if personally delivered, when delivered; or
- (b) if posted, three Business Days after posting (provided that any notice received after 5:00 p.m. or on a day which is not a Business Day will be deemed not to have been received until the next Business Day); or
- (c) if sent electronically (including by email or by an electronic application), on the Business Day it is sent, or the next Business Day if sent outside normal business hours, (provided that the electronic communication was correctly addressed to the address provided by the addressee for the receipt of electronic communications and no error message was received by the information systems used by the sender to send the electronic communication).

27.4 Proof of electronic service

In proving service of a notice and any accompanying documents sent electronically it is sufficient to prove that the electronic communication was properly addressed and that a delivery-receipt message was received by the person who sent the electronic communication.

28. General

28.1 Severance

The illegality, invalidity, or unenforceability of any provision in these Terms will not affect the legality, validity, or enforceability of any other provisions.

28.2 Employees, representatives and contractors

Each API Standards User must ensure its employees, representatives, agents, and contractors comply with, and fulfil the obligations of an API Standards User set out in, these Terms.

28.3 Third party rights

Subject to the indemnities given, and exclusions and limitation of liability, in these Terms (which may be relied on and enforced by the relevant indemnified party), a person who is not a party will not have any rights under or in connection with these Terms or the API Centre Agreement by virtue of the Contract and Commercial Law Act 2017.

28.4 No agency

These Terms do not create any relationship between the parties of principal and agent, partnership, joint venture, or employer and employee. Neither party will have authority to act for or incur any obligation on behalf of another party, except as expressly provided for in these Terms.

28.5 Remedies cumulative

The rights and remedies provided in these Terms are cumulative and not exclusive of any rights or remedies provided by these Terms or law.

28.6 Survival

Following termination or expiry of these Terms, this clause 28, and other provisions that are by their nature intended to survive, including clauses 15, 17, 18, 19, 20, 21, 22, 24, and 26, will remain in full force and effect.

28.7 Entire agreement and Precedence

- (a) The documents identified in paragraph (b) below contain the whole of the contract and understanding between the parties in respect of the matters covered by it and supersede all prior representations, agreements, statements and understandings between the parties in respect of those matters, whether verbal or in writing.
- (b) In the event of any conflict of meaning or ambiguity, the following documents have the order of precedence set out below:
 - (i) the Terms; and
 - (ii) the API Centre Agreement.

28.8 Waiver

- (a) A delay, neglect or forbearance by a party in enforcing any provision of these Terms against another party will not waive or limit any right of that party.
- (b) No provision of these Terms will be considered waived by a party unless that party waives the provision in writing.
- (c) The parties will not treat a waiver by a party of any breach as a waiver of any continuing or re-occurring breach, unless the parties have expressly agreed to do so in writing.

28.9 Governing law and jurisdiction

These Terms will be governed by and construed in accordance with New Zealand law. The parties submit to the non-exclusive jurisdiction of the courts of New Zealand.

Appendix 1 — Registration Criteria

Registration Criteria for a Third Party

Requirement for Third Party Registration	
Requirement	
Must have a New Zealand Bank Account.	
Must have a New Zealand GST number.	
Must have a genuine business interest in the use of APIs developed using the API Standards.	

Registration Criteria for an API Provider

Requirement for API Provider Registration	
Requirement	
Must be a NZ registered bank OR a NZ non-bank deposit taker OR an entity prudentially regulated by the Reserve Bank of New Zealand or the Financial Markets Authority New Zealand.	
Must issue and provide bank accounts to its customers using the Payments NZ standard for bank account formats.	
Must have a genuine business interest in the use of APIs developed using the API Standards.	

Registration as an API Provider and Third Party

An applicant who satisfies the Registration Criteria for an API Provider automatically satisfies the Registration Criteria for a Third Party.

Appendix 2 — Third Party Cap on Liability

The cap on liability for third parties (based on tier of membership) pursuant to clause 21.6 is as follows:

Tier	Third Party Category	NZ Turnover	Liability Cap
1	Large third party	\$50m +	\$7,000,000
2	Medium third party	\$15-50m	\$4,000,000
3	Small third party	\$2.5-15m	\$2,000,000
4	Start-up third party	<\$2.5m	\$1,000,000